

**APPLICATION**

**FOR**

**UNITED STATES LETTERS PATENT**

---

**SPECIFICATION**

**TO ALL WHOM IT MAY CONCERN:**

Be it known that I, John S. Erickson, have invented

**System and Methods for Managing Digital Creative Works**

of which the following is a specification.

# System and Methods for Managing Digital Creative Works

## Related Applications

This application is a continuation-in-part of U.S. Patent Application No. 08/543,161, entitled "System and Methodology for Protecting Copyrighted Electronic Media," filed on October 13, 1995, and is a continuing application of Provisional Application No. 60/025,485, filed on August 29, 1996, both of which are expressly incorporated herein by reference.

## Background of the Invention

The management of copyrighted material in the prior art is largely based upon hard copy technology, which attaches attribution and notification to creative works, such as copyright notices, by lines and credits. This technique is prone to significant error because notices become outdated, removed and/or ignored. Further, any copyright violation of the hard copy creative work - such as physical, unlawful copying of an article on a copying machine - is difficult to determine.

Digital media exacerbate these problems. Specifically, copyright infringement and theft has increased enormously in the computer age, particularly with respect to information data transfers through the Internet. Further, electronic email and the communication and connectivity of local and wide area networks (LANs and WANs, respectively) have facilitated unauthorized use of copyrighted materials by permitting tagging and/or enclosing of almost any electronic media, such as application software, authored text files and graphics, and musical sounds.

On-line services such as Compuserve™ and America Online™ do provide some measure of copyright protection by assessing on-line charges to the access of protected databases and to the download of selected files. However, there is little to

1 prevent that on-line user from retransmitting any downloaded files to another user  
2 connected on the Internet. If the user is also connected to a network, those  
3 downloaded files are also subject to remote access from yet another unauthorized  
4 user.

5  
6 The problems associated within electronic copyright infringement are well  
7 known, particularly by those parties injured by the unauthorized use of copyrighted  
8 materials. For example, the unauthorized copying of copyrighted magnetic diskettes,  
9 and the electronic email and tagging and/or enclosing of copyrighted files can  
10 result in a direct monetary loss to the owner of the copyrighted works, in addition  
11 to an unaccounted for gain for the unauthorized user. With the expansion of the  
12 Internet and other computerized networks, the aggregate amount of such losses and  
13 gains is substantial.

14  
15 Even the U.S. Commerce Department recognizes that serious copyright  
16 problems exist with the burgeoning growth of electronic data transfers between  
17 networked computers and particularly through the Internet. Early in September  
18 1995, for example, the Commerce Department issued a white paper entitled  
19 "Intellectual Property and the National Information Infrastructure." The paper  
20 highlights the need to protect copyrighted information that is resident in cyberspace,  
21 where unauthorized users can copy original works of authorship, including movies  
22 and books, by pressing a couple of keystrokes. See, V. Sussman, Copyright wrong? A  
23 fight brews over who gets to own the future (cyberspace), U.S. News & World  
24 Report, September 18, 1995, v119 n11 p99(1).

25  
26 In the prior art, methods have been developed to enhance copyright  
27 protection of electronic media. For example, AT&T Bell Laboratories has developed  
28 a system which makes tiny adjustments to the spacing between words so that every  
29 copy of a document utilizing the system is "unique." These electronic adjustments  
30 are detectable by computers only because they are too small for the human eye to

1 notice. By way of another example, Digimarc, a company in Portland, Oregon,  
2 recently announced a system that encodes data into an image by carefully adjusting  
3 the digital representation of individual pixels. As in the AT&T system, the encoded  
4 data is not noticeable to the eye and enables some traceability of unauthorized  
5 copyright uses. See, S. Steinberg, editor of Wired Magazine, Los Angeles Times  
6 column, p2, part D, August 31 (1995).

7  
8 However, such systems operate only to detect unauthorized usage of  
9 copyrighted works in digital form. They do not manage the access to copyrighted  
10 works, nor do they provide any systematic way of controlling the rights to  
11 copyrighted electronic media.

12  
13 More particularly, the tracing of copyright clearances to users of copyrighted  
14 electronic media in the prior art is a tedious and often impossible task. Specifically,  
15 authors and multimedia developers have had only two practical methods for  
16 protecting their copyrights of electronic works: one method is to rely upon copyright  
17 laws and international treaties to prohibit unauthorized use of the media; and the  
18 other is to encrypt the data, so that access is restricted to those users with a  
19 decryption key.

20  
21 In the first method, media developers typically do nothing; or they attach a  
22 textual copyright warning - sometimes called a "watermark" - to the media. This  
23 type of "protection" ensures free access to the media, but it works only for those  
24 honest users and derivative developers who view the work and decide whether they  
25 want to license it. However, users and developers of such media cannot be sure of  
26 the authorship or integrity of the media. Authenticity is thus sometimes increased by  
27 restricting access to the media, such as through the use of a password. By way of  
28 example, a password-protected World Wide Web page provides some measure of  
29 authenticity, but also discourages the open and free propagation of the information  
30 in the media.

1  
2 In the second method, media developers can utilize powerful encryption  
3 tools, readily available in the public domain, such as those tools based on the RSA  
4 public key algorithm (Rivest, Shamir, & Adleman, 1977). However, the use of  
5 encryption to protect copyrights only serves to restrict access to the information  
6 within the media, like the password described above. Moreover, after the work is  
7 decrypted on the recipient's computer, the problems of copyright heritage and  
8 permissions for derivative development and use of the media remain.

9  
10 These two methods favor either the user or the owner of the media. In the first  
11 method, for example, there is no electronic protection coupled to the media; and it  
12 thus favors the free and fair use of the media at the expense of the owners' rights. On  
13 the other hand, the second method of encryption favors the owners' rights, at least to  
14 a degree. Neither method affords both fair use and ownership protection; and  
15 neither provides for automatic management of media rights, including the  
16 controlled access to media in derivative works. Further, these methods do not  
17 intervene in managing copyrights, and are beneficial only after the copyright issue  
18 becomes a problem.

#### 19 20 Objects of the Invention

21  
22 It is one object of the invention to provide systems and methodologies to  
23 protect the rights of intellectual property owners while promoting open and free  
24 sharing of information.

25  
26 Another object of the invention is to provide methods for ensuring that  
27 benefits owed to owners, publishers and creators of creative works accrue to such  
28 entities.

1 Still another object of the invention is to provide methods and systems for  
2 crediting authors, publishers and creators of electronic multimedia objects that  
3 include digital creative works.

4  
5 Other objects of the invention provide tools to acquire, publish, distribute,  
6 and disseminate multimedia objects to strengthen ownership and attribution of the  
7 underlying digital creative work.

8  
9 Another object of the invention provides systems and methods for packaging  
10 and unpackaging digital creative works within a data container to facilitate the  
11 management of that work.

12  
13 Another object of the invention provides systems and methods for attaching  
14 copyright notices and other attributes to digital creative works.

15  
16 Other objects of the invention provide for (a) locating source works of  
17 derivative authors of digital creative works, (b) obtaining releases and permissions  
18 to incorporate another work or part of another work into the digital creative work,  
19 (c) determining the source and attributes of digitally creative works, (d) promotion  
20 of communication directly to the author or owner of the digital works, (e) security  
21 and authentication of transactions and the digital work, and (f) the automation of  
22 rights management, such as acquisition, administration, and authorization of digital  
23 creative works.

24  
25 It is still another object of the invention to provide systems and  
26 methodologies to manage copyrighted electronic media, thereby solving or reducing  
27 the problems of the prior art.

28

1 Yet another object of the invention is to provide a method for maintaining an  
2 electronic bibliographic record of successive data transfers of protected electronic  
3 media.

4  
5 Still another object of the invention provides systems and methods for  
6 packaging and unpackaging electronic media within an electronic container to  
7 facilitate the management of copyrighted electronic media.

8  
9 These and other objects of the invention will be apparent from the description  
10 which follows.

#### 11 12 Summary of the Invention

13  
14 As used herein, a "copyrighted work" means any work that is authored and  
15 protected by U.S. and international copyright laws, including, without limitation,  
16 literary works; musical works, including any accompanying words; dramatic works,  
17 including any accompanying music; pantomimes and choreographic works;  
18 pictorial, graphic, and sculptural works; motion pictures and other audiovisual  
19 works; sound recordings; and architectural works. "Electronic media" means any  
20 electronic form or digital representation of a copyrighted work.

21  
22 As used herein, a "Digital Creative Work" means any electronic media,  
23 multimedia content element, electronic creative work, and in particular work such as  
24 authored and protected by U.S. and international copyright laws, including, without  
25 limitation, any of the following in digital or electronic form: literary works; musical  
26 works, including any accompanying words; dramatic works, including any  
27 accompanying music; pantomimes and choreographic works; pictorial, graphic, and  
28 sculptural works; motion pictures and other audiovisual works; sound recordings;  
29 and architectural works. Further, a Digital Creative Work can include multimedia  
30 content elements that have two or more creative works, such as a digital image and

1 associated digital audio. As such, a Digital Creative Work includes any electronic  
2 form or digital representation of a copyrighted work, including multimedia objects,  
3 and including any form or digital representation (1) stored within computer memory  
4 or other electronic memory, (2) resident on CD-ROM and/or magnetic disk or tape,  
5 (3) transmitted as a digital file through email, an on-line service such as  
6 Compuserve™, the World Wide Web (WWW), Intranet and/or the Internet; and (4)  
7 communicated as a digital file within or into a computer network, such as a LAN or  
8 WAN, and including any communication obtained through remote access. Further, a  
9 Digital Creative Work can include, but is not limited to, digital embodiments of a  
10 creative expression, such as digital audio (eg: WAV, SND, AIFF, AU), digital music  
11 sequences (eg: MIDI), digital video (eg: AVI, MOV, MPEG), digital images and  
12 graphics (eg: GIF, BMP, TIFF, JPEG, FlashPix), word processing files (eg: DOC), and  
13 spreadsheet files (eg: XLS).

14  
15 As used herein, "CONTAINER" means an electronic or digital entity that is  
16 constructed according to the invention to enable the use of, control of, access to,  
17 and/or licensing of the Digital Creative Work. The CONTAINER is a logical entity  
18 that is preferably based on object technology such as C, C++, Visual Basic,  
19 Microsoft's ActiveX™ Controls, Microsoft's OLE™ Controls, Apple's OpenDoc™,  
20 and Sun Microsystem's Java™ applet component technologies. Accordingly, a  
21 CONTAINER of the invention is a data container that includes a data portion with  
22 the Digital Creative Work, and an executable portion that typically adds  
23 functionality to Web Sites, desktop applications and development tools in order to  
24 manage that Digital Creative Work. A CONTAINER can be distributed through  
25 many channels, such as through the Internet, CD ROM, or magnetic media.  
26 Further, a CONTAINER can be formed of different parts that are located remotely to  
27 one another; though the different parts are linked to maintain attribution within the  
28 CONTAINER.

29

1 As used herein, "METADATA" refers to data associated or encapsulated with  
2 a CONTAINER and includes a plurality of data pertinent to copyright management,  
3 including, for example, ownership identification and contact information, rights  
4 administration identification and contact information, creatorship identification and  
5 contact information, an identification and address of a registration server, listings of  
6 antecedent and related objects, and licensing terms and conditions.

7  
8 As used herein, a "DIGITAL CONTRACT" means a contract secured through  
9 licensing activity between a registration server and a user of a Digital Creative Work.  
10 The Digital Contract includes a textual expression of enhanced permissions for use  
11 of the Digital Creative Work and may or may not be accompanied by an upgrade of  
12 the operational controls such as the ability to print, save and/or edit the Digital  
13 Creative Work.

14  
15 As used herein, "SYSTEM EXTENSION" means an operating system  
16 extension or "plug-in" that each user obtains prior to use and/or manipulation of  
17 one or more CONTAINERS. Specifically, the SYSTEM EXTENSION operates in  
18 conjunction with the operating system of a computer to recognize CONTAINERS  
19 and to permit authorized operations on the CONTAINER's METADATA and/or  
20 Digital Creative Works. When needed, the EXTENSION can and will be  
21 downloaded from various trusted locations and such as described herein so as to  
22 render Digital Creative Works within CONTAINERS. However, the EXTENSION is  
23 generally resident on a user's computer so as to obviate the need to continually  
24 download the EXTENSION and to improve network efficiency.

25  
26 As used herein, "OBJECT" means an instantiation such as an icon, graphic or  
27 other visual, on a computer, which is, or which refers to, or which points to an object  
28 such as a CONTAINER. Typically, an OBJECT is viewable within an application  
29 such as a Web browser such that a user directly views authorized content of the  
30 Digital Creative Work. However, for example, a user can select or "click" the

1 OBJECT with a computer mouse to gain additional information in and to the  
2 CONTAINER and/or to obtain additional licenses to the OBJECT's Digital Creative  
3 Works. The OBJECT thus instantiates the existence of the Digital Creative Work in a  
4 composition such as a CONTAINER. In the usual case, for example, a Digital  
5 Creative Work within a CONTAINER is actually an image (i.e., the "OBJECT") on a  
6 user's computer. In the preferred embodiment of the invention, the user will view an  
7 OBJECT and not notice anything different about the Digital Creative Work until the  
8 user tries to operate on the OBJECT in ways that are prohibited. For example, when  
9 a user attempts to click on the OBJECT, or to print the OBJECT, or to copy the  
10 OBJECT to another file, or to attempt other operations that are restricted, the  
11 EXTENSION takes over and informs the user that such operations are prohibited  
12 without an additional license to the Digital Creative Work. An OBJECT can be  
13 formed of a group of OBJECTS. Once permissions or licenses are granted to perform  
14 additional operations, such as copying, the DIGITAL CREATIVE WORK and  
15 METADATA remain linked during the copying process so that the user copies the  
16 CONTAINER, preserving attribution and facilitating the further management of the  
17 Digital Creative Work. It is important to note that an OBJECT instantiates a  
18 CONTAINER which itself can exist locally, e.g., within internal memory, and/or  
19 remotely across one or more sites on the Internet. The invention communicates an  
20 OBJECT to a user through a file or a continuous data stream: in the first case, the  
21 OBJECT is rendered to the user after the complete data set is received; and in the  
22 second case the OBJECT is rendered as the data is received through the  
23 communication link.

24  
25 As used herein, "TOOL BOX" or "TOOLBOX" means a software application  
26 that is used to create or augment a CONTAINER. Typically, the TOOL BOX is  
27 resident on a computer to facilitate the management of Digital Creative Works from  
28 the author or creator's desktop computer.

29

1       As used herein, "PACKAGER" means an application which creates or  
2       augments a CONTAINER. Typically, the PACKAGER operates in a batch mode and  
3       is used in high-volume generation of CONTAINERS for creators and owners of large  
4       amounts of digital creative works. By way of another example, the PACKAGER can  
5       package HTML documents, i.e., Web pages, so that a user of the Web page is  
6       actually within an OBJECT that is likely composed of other OBJECTs.

7  
8       As used herein, a "VIEWER" refers to software and/or hardware which  
9       renders the Digital Creative Work of a CONTAINER to a user. For example, a  
10      CONTAINER can be associated with a web page that is accessed by users of the  
11      Internet. In order to perceive the CONTAINER, and in particular the Digital  
12      Creative Work associated with the CONTAINER, the user's host computer calls on  
13      the appropriate media "viewer" service registered with the computer's operating  
14      system. If the Digital Creative Work is, for example, a GIF file, the computer tells the  
15      SYSTEM EXTENSION to do the rendering and the SYSTEM EXTENSION, in turn,  
16      calls on a GIF viewer or renderer to display the GIF (i.e., the Digital Creative Work  
17      in this example) to the user. Similarly, a VIEWER can refer to rendering software of  
18      JPEGs, AVIs, PDFs, MIDs, etc. Indirectly, the VIEWER is sometimes embodied with  
19      the SYSTEM EXTENSION or as separate software specific to the invention so as to  
20      render, for example, a Digital Contract. More particularly, when asked by the user  
21      (e.g., with the "click" of a computer mouse), the EXTENSION renders the associated  
22      Digital Creative Works with a VIEWER specifically designed to view the Digital  
23      Contract. The VIEWER also refers to a computer subsystem, operable by a user  
24      desiring to manipulate one or more CONTAINERS that contain either (a) a shell  
25      extension which responds to direct manipulation, at the computer, of OBJECTS  
26      referring to CONTAINERS, or (b) an object control, which is used to display  
27      CONTAINERS - or portions of CONTAINERS - within other applications. By way of  
28      example, an object control of the invention can include ActiveX Control that permits  
29      display of an OBJECT, within an application such as a web browser, that links the  
30      computer to the CONTAINER.

1

2       As used herein, "REGISTRY" generally refers to a registration server that  
3 registers CONTAINERS and which operates to manage Digital Creative Works. A  
4 user of a particular CONTAINER communicates to the REGISTRY via on-line  
5 communication to obtain auxiliary permissions to the Digital Creative Work therein.  
6 The CONTAINER contains information in the METADATA which specifies the  
7 "home" or licensing site assigned to the CONTAINER. By way of example, when a  
8 user clicks on an OBJECT to request auxiliary use of the Digital Creative Work, the  
9 CONTAINER automatically prompts the EXTENSION to locate and connect with  
10 the assigned REGISTRY through Internet communication. In certain aspects of the  
11 invention, the REGISTRY includes a separate registration server and an  
12 authorization server. The registration server is used to register CONTAINERS, and  
13 the authorization server is used to authorize auxiliary uses of CONTAINERS, such  
14 as to provide licensing to the Digital Creative Works therein. However, the  
15 REGISTRY is typically a single registration server that operates as a registration  
16 server and as an authorization server to negotiate licenses with on-line users of  
17 Digital Creative Works.

18

19       In one aspect, the invention applies object technology to the Digital Creative  
20 Work to form a data CONTAINER including the data content of the Digital Creative  
21 Work and other attributes contained in METADATA. These attributes can include  
22 operations, services and information that describe or operate on the METADATA  
23 and/or Digital Creative Work as appropriate to the user according to the minimum  
24 and/or auxiliary permissions granted within the METADATA. In another aspect,  
25 the attributes and content of a CONTAINER are distributed between (a) the local  
26 system, i.e., where a user views and/or manipulates the CONTAINER, and (b) a  
27 registration server to which it refers across the Internet. The registration server  
28 further can contain attributes that, for various reasons such as volatility, security, or  
29 efficiency, cannot or should not travel to the local system.

30

1        In another aspect, a repository system provides file images, i.e., persistence  
2 data, of CONTAINERS as well as resources and data referred to by CONTAINERS  
3 but not held in attributes at the registration server.

4  
5        In one aspect of the invention, a user at a computer accesses a particular  
6 CONTAINER through a set of property pages (e.g., tabbed dialog boxes), or  
7 "templates," that are available through the CONTAINER wherever it appears. For  
8 example, where an OBJECT for a CONTAINER appears in a screen rendering of a  
9 Web browser, a mouse click onto the OBJECT brings up its associated property  
10 pages to show information and to provide access to features such as email and  
11 authentication to the associated digital creative work.

12  
13        In still another aspect, and as described herein, creators or authors of digital  
14 creative works bind content and attributes into a CONTAINER; and register new  
15 CONTAINERS through a locally resident TOOL BOX which facilitates the flexible  
16 design of the CONTAINER's property pages and feature selections. In still another  
17 aspect, the TOOL BOX also automates the organization and maintenance of the  
18 heritage of the Digital Creative Work, such as when the CONTAINER includes  
19 works from various authors.

20  
21        In another aspect, one or more CONTAINERS can be, and preferably are,  
22 registered at the REGISTRY, which preferably is a secured registration server system  
23 remote from the viewing capabilities of the SYSTEM EXTENSION or VIEWER. In  
24 this aspect, the REGISTRY (a) retains information to validate the credentials and/or  
25 authenticity of a TOOL BOX, attempting to register a work, or a CONTAINER; and  
26 (b) supplies remote services and data. The REGISTRY can also supply attribute data  
27 obtained indirectly from a content provider's existing legacy database.

28  
29        In accord with preferred aspects of the invention, access to OBJECTS is  
30 generally "open" such that any user can view the associated Digital Creative Work.

1 The SYSTEM EXTENSION in this aspect is thus ubiquitous, as are most or all  
2 supplementary VIEWERS. That is, when a VIEWER is called by the EXTENSION,  
3 the invention preferably utilizes handshaking standard such as Microsoft's code  
4 signing standard. Such a standard uses digital signature technology that helps one  
5 application make sure that it is talking to the authentic version of another  
6 application. Accordingly, the SYSTEM EXTENSION in this aspect is sure to call the  
7 correct VIEWER and not some other viewer that does damage to the DIGITAL  
8 WORK or CONTAINER.

9  
10 In one aspect, the invention provides a method of packaging a digital creative  
11 work, including the steps of: encapsulating the work within a data container;  
12 encapsulating metadata within the container; and integrating, with the container,  
13 means for accessing the work and the metadata. In another aspect, the step of  
14 integrating further comprises the step of integrating, with the container, means for  
15 rendering the work. The method can also include any of the following steps:  
16 integrating, with the container, means for printing the work; integrating, with the  
17 container, means for copying the work; integrating, with the container, means for  
18 viewing the work; integrating, with the container, means for controlling use of the  
19 work; integrating, with the container, means for limiting use of the work;  
20 integrating, with the container, means for disallowing use of the work; integrating,  
21 with the container, means for operating on the metadata; integrating, with the  
22 container, means for providing email to one or more external addresses; integrating,  
23 with the container, means for providing web access to one or more WWW addresses;  
24 integrating, with the container, means for providing interactive licensing to the  
25 work; integrating, with the container, means for providing a link to a digital contract  
26 for the work; integrating, with the container, means for updating the metadata; and  
27 integrating, with the container, means for displaying descriptive information.

28  
29 The descriptive information can include one or more of the following:  
30 authorship information, historical information, ownership information, date

1 information, time information, and bibliographic information. It can further include  
2 a digital signature to verify authenticity of the work.  
3

4       The method of the invention can also include the step of forming the data  
5 container as a plurality of associated data that are distributed across one or more of  
6 the following: a computer network, the Internet, a LAN, a WAN, an on-line service,  
7 and an Intranet. Further, the work can be selected from the group of digital images  
8 and graphics, digital photos, digital audio, digital video, digital music sequences,  
9 word processing files, spreadsheet files, and mixtures thereof. For example, the  
10 digital images and graphics can include JPEG, GIF, BMP, TIFF and mixtures thereof.  
11 Similarly, the digital audio can include WAV, SND, AIFF, AU and mixtures thereof.  
12 Further, the digital music sequence can include MIDI; and the digital video can  
13 include AVI, MOV, MPEG and mixtures thereof. The word processing programs can  
14 include, among others, Microsoft Word™, Novell WordPerfect™ and mixtures  
15 thereof. Likewise, the spreadsheet programs can include, among others, Microsoft  
16 Excel™.  
17

18       The step of encapsulating metadata can include the step of encapsulating  
19 copyright management information. The copyright management information can  
20 include any of ownership identification information, ownership contact information,  
21 rights administration information, rights administration contact information,  
22 creatorship information, authorship information, creator contact information, author  
23 contact information, listings of antecedent object information, listings of related  
24 object information, licensing terms, licensing conditions, publisher information, and  
25 ownership credits. These can further include email addresses, web access addresses,  
26 and mixtures thereof. The step of encapsulating metadata can further include the  
27 step of encapsulating registration data, the registration data identifying an  
28 associated registration server capable of administrating the data container.  
29

1 Preferably, the metadata is modifiable and accessible through on-line  
2 communication with the registration server. Accordingly, the method can include  
3 the step of storing at least part of the metadata at a database of the registration  
4 server, or the step of down-loading at least part of the metadata from the registration  
5 server.

6  
7 The methods of the invention can also include the step of providing a user  
8 interface to the data container to review at least part of the metadata on a computer.  
9 The user interface is preferably displayable on the computer and is selectable by a  
10 user of the computer to modify information therein.

11  
12 In another aspect, the step of encapsulating metadata further includes the step  
13 of encapsulating, with the data container, minimum permissions data, the minimum  
14 permissions data specifying one or more operations that can be performed on the  
15 work without a license to the work.

16  
17 In still another aspect, the step of encapsulating metadata further includes the  
18 step of encapsulating, with the data container, minimum permissions data, the  
19 minimum permissions data specifying a default contract to the work, the default  
20 contract specifying a minimum set of operations that can be performed by  
21 applications on the work. Such operations, for example, include drag and drop  
22 operations, printing operations, editing operations, activating operations, saving  
23 operations, and viewing operations.

24  
25 The step of integrating means for accessing the work and the metadata can  
26 include the step of integrating, with the container, one or more of the following:  
27 means for encoding the metadata, means for compressing the metadata, means for  
28 manipulating the metadata, means for encrypting the metadata, means for decoding  
29 the metadata, and means for decrypting the metadata. Similarly, the step of  
30 integrating means for accessing the work and the metadata can include the step of

1 integrating, with the container, one or more of the following: means for encoding the  
2 work, means for compressing the work, means for manipulating the work, means for  
3 encrypting the work, means for decoding the work, and means for decrypting the  
4 work.

5  
6 In another aspect, the step of encapsulating the work further includes the step  
7 of encrypting the work. Alternatively, the step of encapsulating metadata can  
8 include: the step of associating a metadata template with the container, the metadata  
9 template describing registration with a registration server; or the step of associating  
10 a metadata template with the container, the metadata template specifying properties  
11 of the container used to register the container with a registration server. A further  
12 step can include specifying, within the template, a display interface used to view the  
13 properties.

14  
15 In another method of the invention, the step of encapsulating metadata  
16 includes the step of associating a metadata template with the container, the metadata  
17 template identifying user-selectable optional properties of the container. Further, the  
18 step of encapsulating metadata can include the step of associating a metadata  
19 template with the container, the metadata template specifying requirements and  
20 rules associated with the work.

21  
22 Certain aspects of the invention include providing, with the metadata  
23 template, a user interface suitable for viewing information related to the metadata  
24 and the work; and/or providing different metadata templates corresponding to  
25 different types of works; and/or providing different metadata templates  
26 corresponding to different licensing models.

27  
28 One method of the invention includes, with the step of encapsulating  
29 metadata, the step of associating, with the container, operations that can be  
30 performed on the work.

1  
2 In still another aspect, each registration server provides on-line  
3 administration of the container and has user-selectable registration templates for  
4 associating metadata with the container, at least part of the metadata being  
5 modifiable over a lifetime of the container.  
6

7 Further, the step of encapsulating metadata can include the step of  
8 associating, with the container, requirements of specific parties having rights in or to  
9 the work. The requirements can include a requirement to obtain a license to the  
10 work prior to additional use of the work. The requirements can also include a  
11 requirement of obtaining information about entities desiring access to the work.  
12 Such information can include address and billing information of the entities. The  
13 entities can include one or more of an individual, a partnership, a company, a  
14 government agency, and an educational institution.  
15

16 In another aspect, the step of encapsulating metadata can include the step of  
17 encapsulating information indicative of one or both of an owner and creator of the  
18 media, and further include the step of communicating with one or both of the owner  
19 and creator through one or both of email and web page access. The steps of  
20 encapsulating can be made through object-based technology. Typically, the  
21 container is formed with object-based technology such as of OLE™, ActiveX™,  
22 OpenDoc™, and hybrid OLE™/OpenDoc™.  
23

24 The invention also provides a method of accessing a digital creative work,  
25 including: installing a system extension onto a computer, the extension including (i)  
26 means for operating in conjunction with an operating system controlling the  
27 computer; (ii) means for accessing a data container having the work and metadata,  
28 including minimum permissions data, attached thereto, the minimum permissions  
29 data specifying one or more operations that can be performed on the work without a  
30 license to the work; and (iii) means for recognizing the minimum permissions data

1 and for enabling a user of the computer to use the work in accord with the specified  
2 operations; and accessing the container and using the work in accord with the  
3 specified operations.

4  
5 The step of installing a system extension can include the step of distributing  
6 the extension to the computer with a computer operating system; and/or the step of  
7 distributing the extension to the computer from one or more content provider sites,  
8 the content provider sites creating the media; and/or distributing the extension to  
9 the computer with creativity tools; and/or utilizing image and graphic creativity  
10 tools selected from the group of Adobe Photoshop™, Fractal Design Painter™,  
11 CorelDraw; and/or utilizing multimedia authoring tools selected from the group of  
12 Macromedia Director™, Macromedia Authorware™, Asymetrix Toolbook™,  
13 Aimtech IconAuthor™; and/or utilizing web authoring tools selected from the  
14 group of Microsoft FrontPage™, Adobe PageMill™, Adode SiteMill™, SoftQuad  
15 HoTMetaL Pro™, Corel Web.Designer™; and/or utilizing sound editing tools  
16 selected from the group of Macromedia SoundEdit Pro™ and DigiDesign Pro  
17 Tools™; and/or utilizing video editing tools selected from the group of Avid Media  
18 Suite™, Asymetrix Digital Video Producer™, Adobe Premiere™; and/or  
19 distributing the extension to the computer with web browsers selected from the  
20 group of Netscape Navigator™ and Microsoft Internet Explorer™.

21  
22 By way of example, the creativity tools of the invention can include one or  
23 more of the following: Microsoft Word™, Microsoft Excel™, Microsoft  
24 Powerpoint™, and Novell WordPerfect™.

25  
26 In another aspect, the container is stored in a remote database, and the  
27 methods of the invention include the step of accessing at least part of the container  
28 through on-line communication with the database. For example, the step of  
29 accessing part of the container through on-line communication can include one or  
30 more of the following: communication through the Internet, communication through

1 a computer network, and communication through the Intranet; and/or utilizing a  
2 file data stream wherein rendering of the work is possible only after all data  
3 representative of the work is present at the computer; and/or utilizing a continuous  
4 data stream wherein rendering of the work is possible, in part, with concurrent  
5 arrival, at the computer, of data representative of the work.

6  
7 In one aspect, the container is stored on a CD-ROM, and the method includes  
8 the step of accessing that part of the container through communication with a CD-  
9 ROM drive. Alternatively, for example, the container is stored on a magnetic data  
10 disk, and the invention includes the step of accessing part of the container through  
11 communication with a disk drive. In still another example, the container is stored  
12 within internal memory of the computer, and the method includes the step of  
13 accessing part of the container within internal memory.

14  
15 In still another aspect, the system extension includes means for recognizing  
16 registration data within the metadata, the registration data identifying an associated  
17 registration server capable of administrating the data, and the method includes the  
18 step of contacting the registration server to negotiate, on-line, a license to the work.  
19 An additional step can include contacting the registration server to negotiate for  
20 auxiliary permissions data, the auxiliary permissions data specifying auxiliary uses  
21 of the media that is licensed beyond the authorized use specified in the minimum  
22 permissions data.

23  
24 In another aspect, the extension can include: means for recognizing the  
25 auxiliary permissions data and for enabling the user to use the work in accord with  
26 the auxiliary uses; and/or means for recognizing registration data within the  
27 container, the registration data identifying an associated registration server capable  
28 of administrating the data, and can further include the step of contacting the  
29 registration server to authenticate the work; and/or means for prohibiting  
30 unauthorized uses of the work when the unauthorized uses exceed the operations

1 specified in the minimum permissions data. Such unauthorized uses of the media  
2 can include, for example, drag-and-drop operations on the computer, copying,  
3 saving and/or printing the work.

4  
5 Typically, the auxiliary permissions specify a set of operations that can be  
6 performed on the work after executing a digital contract to the work. The auxiliary  
7 permissions are usually obtained through one of email or web access.

8  
9 The invention also provides improvements to an operating system of the type  
10 which facilitates control and communication of a digital data processor. A plug-in  
11 extension is used to manipulate copyrighted electronic media, the extension having  
12 means for opening a data container having a digital creative work and minimum  
13 permissions data attached thereto. The minimum permissions data specifies one or  
14 more operations that can be performed on the work without a license to the work.  
15 The extension recognizes the minimum permissions data and enables a user of the  
16 processor to use the work in accord with the specified operations.

17  
18 The container can also have metadata attached thereto. The metadata  
19 typically has one or more of ownership identification information, ownership  
20 contact information, rights administration information, rights administration contact  
21 information, creatorship information, authorship information, creator contact  
22 information, author contact information, listings of antecedent object information,  
23 listings of related object information, licensing terms, licensing conditions, publisher  
24 information, and ownership credits, and wherein the extension comprises means for  
25 reviewing the metadata selectively.

26  
27 In another aspect, the invention provides a plug-in operating system  
28 extension, including: means for operating in conjunction with an operating system  
29 controlling a digital data processor; means for recognizing a data container having  
30 digital creative works and minimum permissions data attached thereto, minimum

1 permissions data specifying one or more operations that can be performed on the  
2 work without a license to the work; and means for opening the container and  
3 enabling a user of the processor to use the work in accord with the specified  
4 operations.

5  
6 In this aspect, the container can have registration information attached  
7 thereto, the registration information specifying a registration server capable of  
8 administering the container, and can further include means for recognizing the  
9 registration information and for communicating with the registration server to  
10 acquire properties associated with the container:

11  
12 The container can have registration information attached thereto, the  
13 registration information specifying a registration server capable of administering the  
14 document, and can include means for negotiating a digital contract with the  
15 registration server, the contract specifying licensing terms and auxiliary uses to the  
16 work.

17  
18 In still another aspect, a server is provided for managing digital copyrighted  
19 works, including: (A) means for communicating with at least one on-line data  
20 processor connected for communication with the server, the on-line data processor  
21 having (i) means for recognizing a secure digital document having copyrighted  
22 electronic media and minimum permissions data attached thereto, the minimum  
23 permissions data specifying minimum authorized use of the media without a license  
24 to the media; and (ii) means for opening the document and enabling a user of the  
25 processor to use the media in accord with the authorized use; (B) means for  
26 registering the document according to user-selected options at the data processor;  
27 and (C) means for negotiating with the data processor to obtain auxiliary  
28 permissions to the document and for sending the auxiliary permissions data to the  
29 data processor thereby expanding the authorized use of the data processor.

30

1       The invention thus provides several advantages. By way of example, it  
2 provides for identification of digital creative works so that potential licensees know,  
3 or can learn of, the owner, author, creator, and publisher of the underlying digital  
4 work. In accord with the invention, the use of the container, based in object  
5 technology, with METADATA and the Digital Creative Work attached thereto  
6 facilitates the appropriate identification of the Work. The METADATA provides the  
7 vehicle for identification information and minimum permissions to the Work, and  
8 further provides detail for subsequent licensing of the Work. Further, the invention  
9 permits substantially seamless interaction between users and the Digital Creative  
10 Work. By way of example, OBJECTs appear like any other visual instantiation on a  
11 web page. It is only after the user tries to operate on the OBJECT beyond the user's  
12 current consumption, e.g., viewing the OBJECT on the computer screen, when it  
13 becomes apparent that there is additional control associated with the OBJECT.

14  
15       The invention also provides for the secure electronic copyright management  
16 and automatic identification of ownership of creative works distributed as digital or  
17 electronic media, particularly over computer networks. Briefly, one aspect of the  
18 invention provides a system which packages electronic media into a secure  
19 document format (the "CONTAINER"), including a data container for the media  
20 and a minimum permissions data set to specify the minimum authorizations needed  
21 to view or otherwise access the media. The CONTAINER can also include a  
22 container header, a container identifier, a source works extensions module which  
23 maintains a bibliographical history of the media, and a digital signature to  
24 authenticate the media. The CONTAINER and the associated network-based tools,  
25 described below and constructed according to the invention, enable the attachment  
26 of minimum permissions to copyrighted works and the subsequent on-line licensing  
27 of the media.

28  
29       More particularly, and in another aspect of the invention, the CONTAINER  
30 containing the media is registered on a registration server and licensed through an

1 authorization server (together the "REGISTRY"). Potential licensees view the  
2 CONTAINER through the authorizations within the minimum permissions data set,  
3 and communicate with the authorization server, if desired, to obtain a license to the  
4 media. Once licensed, the licensee can utilize the media in accord with an auxiliary  
5 permissions data set that is assigned to the CONTAINER during the on-line  
6 licensing transaction.

7  
8 Subsequent viewers and/or users of the CONTAINER also communicate  
9 with the authorization server. Thus, in another aspect, the invention provides for the  
10 licensing of the media to creators of derivative works, i.e., those who modify an  
11 original work of authorship and who obtain authorization to do so through an  
12 augmentation in the permissions data set. As above, the modified CONTAINER is  
13 then registered on a registration server and licensed through an authorization server.  
14 The CONTAINER in this aspect preferably includes a sourceworks extension  
15 module which records the original and derivative authorship of the media. By  
16 retaining such information, a copyright "family tree" or electronic bibliographic  
17 record is maintained for the media. Preferably, the authorship information in the  
18 sourceworks extensions is resident as a data element within the CONTAINER.  
19 However, the sourceworks extensions can also be maintained on or through the  
20 authorization servers, depending upon the number of servers used in the  
21 registration of derivative uses of the media.

22  
23 Like the sourceworks extensions, the invention can also record any and all  
24 users who access the media. In accord with this aspect, the CONTAINER includes a  
25 usage module which records selected information about each user who accesses the  
26 media. The selected information can include, for example, a unique address of the  
27 user, individual or company accessing or utilizing the media, or the actual identity  
28 of the user. Preferably, the user information stored in the usage module is recorded  
29 and stored only after auxiliary permissions are augmented to the minimum  
30 permissions data set; and typically, the user's identity or location is recorded in the

1 course of the licensing transactions with the authorization server. Like the  
2 sourceworks extensions, the usage module can also be resident with the  
3 CONTAINER, as another data element, and/or with the authorization server. In the  
4 latter case, each time a user communicates with an authorization server to license a  
5 particular media, the user's identity or location are recorded and stored therein.  
6

7 Accordingly, the invention provides several advantages in the automation  
8 and tracing of copyright clearances for both the initial users and derivative  
9 developers of electronic media. Unlike the methods in the prior art - i.e., the method  
10 of relying on copyright laws and treaties to protect copyrighted works, and the  
11 method of encrypting the media through electronic keys - the CONTAINER format  
12 and system architecture of the invention provide for (1) both fair use and ownership  
13 protection; and for (2) automatic management of media rights, including the  
14 controlled access to media in derivative works. Specifically, the system of the  
15 invention attaches certain minimum permissions to a widely-distributed version of  
16 the media packaged as a CONTAINER, thus being generally usable for free personal  
17 use. The CONTAINER creator or author determines these minimum permissions in  
18 the spirit of fair use, and the permissions data set are subsequently updated to an  
19 auxiliary permissions data set through on-line licensing should the user be  
20 interested in more advanced licensing or uses of the media.  
21

22 In other aspects, the invention provides an encrypted electronic signature and  
23 optional data encryption, to enhance or guarantee the authenticity of the entire  
24 work, including authorship. More particularly, in other aspects, the CONTAINER  
25 encapsulates the required data in a secure fashion using encryption; and the digital  
26 signatures are based on message digests resulting from one-way hash functions.  
27

28 In still other aspects, the system of the invention utilizes client/server system  
29 architecture based upon the TCP/IP network protocol standard. Those skilled in the

1 art will appreciate that other network protocol standards can be used without  
2 departing from the scope of the invention.

3  
4 In accord with further aspects of the invention, users can unpackage or  
5 unwrap CONTAINERS through a controlled environment, specifically from within a  
6 compatible application or program extension, i.e., a Plug-in, which can provide the  
7 requisite controls over document use.

8  
9 The invention also provides a set of easy-to-use network-based tools for  
10 registering and administering copyrights of electronic creative works. In one aspect,  
11 for example, a viewing module is provided to view and edit media-packaged  
12 graphic, image, video, audio, and textual objects. This viewing module, referred to  
13 herein as a "VIEWER," is generally required, along with the SYSTEM EXTENSION,  
14 to view and edit Digital Creative Works within CONTAINERS.

15  
16 In still another aspect, a packaging module is provided to encapsulate a  
17 newly created work in a secure, digitally-formatted package - i.e., a CONTAINER.  
18 The packaging module, referred to herein as a "PACKAGER," is particularly useful  
19 to authors, creators and publishers who seek to secure their copyrighted works and  
20 who seek to encapsulate other information with the works, such as authorship,  
21 ownership, minimum permissions, and source works extensions. Accordingly, a  
22 user of the PACKAGER can selectively package such information with the media to  
23 formulate a CONTAINER.

24  
25 In other aspects, a registration server provides registration and authorization  
26 services on a platform such as Windows NT or Unix. The registration server is used  
27 by information creators who want users of their works to easily identify ownership  
28 and potential licensing terms, and to transact and license those works on-line. The  
29 Authorization server, on the other hand, is used by information creators and users to  
30 obtain access to Digital Creative Works and to license those works for their own use.

1 Typically, in accord with another aspect, the registration server for each  
2 CONTAINER operates as the authorization server for all subsequent licensing  
3 transactions to that CONTAINER. In this latter aspect, the combination registration  
4 server and authorization server is a REGISTRY.

5  
6 The invention provides certain other advantages over the prior art in that  
7 creators and publishers of electronic media have direct control of the copyrights they  
8 hold through the use of authorization and registration servers. Further, the  
9 invention is preferably compatible with widely accepted object technology  
10 standards, e.g., OLE and OpenDoc, to ensure compliance with the widest possible  
11 range of applications and on several platforms.

12  
13 The invention also provides for automated and controlled network-based  
14 copyright management. The registration server can be scaled to fit the needs of any  
15 authorization and registration service, from single-author shops to massive  
16 centralized clearinghouses.

17  
18 In still another aspect, the VIEWER provides a mechanism for users to gain  
19 access to the data within copyrighted CONTAINERS. Specifically, the VIEWER and  
20 SYSTEM EXTENSION ensure that operations performed on media-packaged data  
21 objects are in compliance with the permissions that have been granted to the user.

22  
23 In other aspects, a user can transact a license to the CONTAINER through on-  
24 line communications with the REGISTRY. More particularly, the SYSTEM  
25 EXTENSION in this aspect (i) generates a licensing request signal in response to  
26 inputs by the user, and (ii) communicates that signal to the authorization server  
27 assigned to that CONTAINER. This request, sometimes denoted herein as a "License  
28 Request," provides an entry point for on-line licensing of media-packaged works. In  
29 this way, a successfully licensed user can obtain auxiliary permissions to the

1 CONTAINER of interest, thereby extending the set of operations which the user may  
2 perform for a given work.

3

4 In still other aspects, the SYSTEM EXTENSION operates to display selected  
5 registry information about the CONTAINER. This display, sometimes denoted  
6 herein as the "Registry Information Display," provides information such as  
7 authorship, ownership, and the licensing terms associated with the electronic media,  
8 thereby facilitating the user's review and evaluation of the CONTAINER prior to  
9 licensing. The registry information is preferably stored in the CONTAINER itself,  
10 and/or at the CONTAINER's registration server.

11

12 A record of the media source works is also available through the SYSTEM  
13 EXTENSION, in accord with another aspect of the invention. As discussed above,  
14 the sourceworks extensions provide a bibliography of the authors of the media so  
15 that the appropriate authors are credited with their works even after the works are  
16 edited by a derivative author. The sourceworks extensions are typically available  
17 within a display - sometimes denoted herein as the "Source Works Display" - at the  
18 user's computer terminal.

19

20 In accord with other aspects of the invention, the SYSTEM EXTENSION  
21 provides standardized tools and procedures for obtaining a certified digital  
22 identification of a CONTAINER, and for becoming a licensed user to that  
23 CONTAINER.

24

25 In another aspect of the invention, a PACKAGER encapsulates authorship,  
26 ownership, minimum use permissions, source works information and the associated  
27 creative works in a secure package. The PACKAGER has several aspects, including:

28

- 29 • Through the PACKAGER, a user can display the status of permissions for  
30 each source work, obtain authorship, ownership, and licensing

1 information from the source work's registration server, and selectively  
2 obtain auxiliary permissions as required for each source work.

- 3 • The PACKAGER allows the author to check clearances for all sources of a  
4 work in progress and to engage in EXTENSION-like licensing transactions  
5 to obtain or upgrade auxiliary permissions.
- 6 • The PACKAGER allows the author to verify and modify the information  
7 that is encapsulated with the packaged media in a CONTAINER.
- 8 • Registration is the final step in setting up a CONTAINER in accord with  
9 the invention; and the PACKAGER provides a registration client and  
10 procedure for registering a new creative work.
- 11 • Like the SYSTEM EXTENSION, the PACKAGER provides standardized  
12 tools and procedures for obtaining a certified digital identification and for  
13 becoming an authorized user.

14  
15 In another aspect of the invention, a Software Development Kit (SDK) is  
16 provided to enable developers of multimedia applications, games, or multimedia  
17 authoring tools (including applications for content creation) to incorporate VIEWER,  
18 SYSTEM EXTENSION and PACKAGER functionality into their applications.

19  
20 The invention thus facilitates the management of copyrighted works and  
21 ensures that the media packaged within a CONTAINER is authentic. The invention  
22 further enables the packaging of useful and selective information with the creative  
23 work, such as container identification, ownership, permissions, and sourceworks  
24 extensions. These features are provided, at least in part, by the VIEWER, SYSTEM  
25 EXTENSION, PACKAGER and the REGISTRY. Through the registration server, for  
26 example, information providers of any size can take advantage of rights  
27 management for their creative works, and users on a network connected to the  
28 server enjoy easy and secure on-line licensing of the works managed therein.

1 In accord with a preferred aspect of the invention, the VIEWER, SYSTEM  
2 EXTENSION and PACKAGER do not impose perceivable overhead during the  
3 course of normal rendering or editing of the work. The execution of VIEWER,  
4 SYSTEM EXTENSION and PACKAGER functionality is quick to ensure that  
5 network functions have good performance within the available network bandwidth.

6  
7 In still other aspects of the invention, VIEWER, PACKAGER, Registration  
8 Server Modules and Authorization Server Modules are operable on Win95,  
9 Windows NT, MacOS and Unix-based platforms.

10  
11 In other aspects, the VIEWER, SYSTEM EXTENSION and PACKAGER of the  
12 invention operate in conjunction with OLE and OpenDoc.

13  
14 The invention also provides a system for authorizing access to copyrighted  
15 electronic media. An authorization server is connected for data transfer between an  
16 internal memory and at least one external data processor, and an internal storage  
17 stores selected information about the electronic media, e.g., the licensing terms for  
18 gaining auxiliary permissions to the media, the copyright ownership of the media,  
19 and revenue estimates about the media. A relay section that is responsive to a  
20 request signal by the data processor communicates the selected information to the  
21 data processor. A data comparison section receives response signals from the data  
22 processor and compares the selected information with the response signals. In this  
23 way, the data comparison section generates an acceptance signal when the response  
24 signals correspond to at least a part of the selected information, and communicates  
25 the acceptance signal to the data processor to authorize access to the media.

26  
27 The system can also store the media within a storage memory, in another  
28 aspect. This memory can be within a computer connected for electronic data transfer  
29 with the data processor, whereby the computer is responsive to the acceptance

1 signal to transfer either (1) authorizations to access the media or (2) the media to the  
2 data processor.

3  
4 The system preferably includes a process section for tagging an encrypted  
5 digital signature to the media, thus authenticating the media. Another section -  
6 including a source works extension module - can also be included to append a  
7 bibliographic record to the media, the bibliographic record forming a digital  
8 representation that specifies information that references each source work and  
9 access restrictions associated with the source work.

10  
11 The system can further include a section for appending auxiliary permissions  
12 to the media, the auxiliary permissions forming a digital representation that specifies  
13 an authorized use of the media, such as viewing, copying or editing the media.

14  
15 In yet another aspect, the system includes an access control section for  
16 withholding access authorization to a portion of the media, the access control section  
17 thus being responsive to the acceptance signal to remove access restrictions to the  
18 portion. In this way, permissions and access to copyrighted media can be provided  
19 to specified parts of a complex multimedia object, e.g., one which includes written  
20 text, graphics and sounds.

21  
22 The invention further provides a system which controls selective access to  
23 electronic media. The system includes one or more servers that communicate via a  
24 data transfer link between an associated system memory containing the media and  
25 at least one external data processor. A communication section communicates  
26 content-specific permission information about the media to the data processor, the  
27 permission information specifying data processor actions which are restricted and  
28 which require augmented access privileges to perform. A storage section enables the  
29 storage of selected other information about the media; while a relay section,  
30 responsive to a request signal by the data processor, communicates the other

1 information to the data processor. A data comparison section receives response  
2 signals from the data processor and compares the other information with the  
3 response signals, the data comparison section generating an acceptance signal when  
4 the response signals correspond to at least a part of the other information. An access  
5 section restricts data transfers between the data processor and a portion of the  
6 media, the access section being responsive to the acceptance signal to remove data  
7 transfer restrictions between the data processor and the portion within the system  
8 memory.

9  
10 The communication section of this aspect can include one of (i) a stand-alone  
11 software module, (ii) a plug-in software module corresponding to an application  
12 environment that generated or modified the media, (iii) a program extension  
13 corresponding to an application environment which generated or modified the  
14 media, (iii) a software module integrated into an application environment by way of  
15 a source code library or linkable object code performing substantially similar  
16 functions.

17  
18 Although other communication protocols are suitable for the invention,  
19 communication standards based upon the TCP/IP network protocol are preferred.

20  
21 The invention also provides methods for authorizing data transfers of  
22 copyrighted digital media, including: affixing content-specific permission  
23 information to the media, the permission information specifying actions which are  
24 restricted and which require augmented access privileges to perform; storing  
25 selected information about the electronic media on an authorization server  
26 connected for data transfer with at least one computer; electronically  
27 communicating selected information about the media to the computer; receiving  
28 response signals from the computer and comparing the selected information with  
29 the response signals; and generating an acceptance signal when the response signals

1 correspond to at least a part of the selected information, thereby authorizing access  
2 to the media.

3  
4 The invention also provides for optional encryption of the data within the  
5 secure container. Accordingly, the methods of the invention include, for example,  
6 the step of encrypting the media through an RSA public key algorithm.

7  
8 The method of this aspect can also include the step of communicating a  
9 digital representation of at least one of (i) a copyright ownership of the media, (ii) a  
10 set of licensing terms for the media for different user classifications, and (iii) revenue  
11 estimates about the media.

12  
13 In another aspect of the invention, a method is provided for maintaining an  
14 electronic bibliographic record of digital media, including: opening an object  
15 container containing the digital media, the object container including a  
16 representation of the media, a data identifier of media, and data specifying  
17 minimum permissions required to access the media; editing the digital media in an  
18 application environment; and attaching the data identifier and minimum  
19 permissions data to the edited media into a source works list. The source works list  
20 provides, among other information, a bibliographic record of the authorship  
21 represented in the media.

22  
23 Such a method can also include the steps of decrypting the media, and  
24 encrypting the media after attaching the data identifier and permissions data into  
25 the source works list.

26  
27 A method of the invention also includes a process for determining the  
28 authenticity of digital media, including the step of affixing an encrypted digital  
29 signature to the media. In this aspect, the CONTAINER is authenticated by encoding  
30 a signature representing the registration of the media. By way of example, a private

1 key is resident with the registration server which is under strict control of the  
2 system. The authenticity - in this example - is thus granted by the registration server  
3 and proven by the digital signature in the CONTAINER. Alternatively, in another  
4 example, the private key is provided to the user of a particular application, again  
5 under the tight control of the system.

6  
7 In yet another aspect, a computer network is provided for managing original  
8 works of authorship, including: a process actuation section for affixing copyright  
9 information to a binary data element corresponding to an authored media; a process  
10 actuation section for affixing minimum permission information to the data element,  
11 the permission information specifying access restrictions to the data element; a  
12 server for storing information concerning the rights to the media, the server  
13 including a control module for controlling access to the data element according to  
14 the minimum permission information by restricting data transfers between the  
15 server and one or more computers networked with the server; a process section for  
16 tagging the data element with supplemental information; and a process section for  
17 maintaining copyright information through derivative uses of data element  
18 throughout the network.

19  
20 The invention also provides a PACKAGER, which is a system for packaging  
21 electronic media within a secure electronic container. The PACKAGER includes a  
22 first process section for attaching a data identifier to the media; and a second process  
23 section for attaching minimum permissions data to the encrypted media, the  
24 minimum permissions data specifying minimum acceptance terms required to  
25 electronically access the media.

26  
27 In other aspects, the PACKAGER includes a process actuation section for  
28 attaching a digital signature to the media, the digital signature providing an  
29 authentication to the media; and a process actuation section for affixing source  
30 works extensions to the media, the source works extensions specifying a

1 bibliographic record of the media. This bibliographic record is a digital  
2 representation that specifies bibliographic information about the authors and  
3 minimum permissions of the media, thereby providing persistence through  
4 generations of derivative use of the media.

5  
6 A SYSTEM EXTENSION and VIEWER subsystem is also provided for  
7 unpackaging electronic media configured within a secure electronic container. A  
8 first process actuation section recognizing permissions data attached to the media,  
9 the permissions data specifying one or more authorizations needed to electronically  
10 access the media; and a second process actuation section opens the media when a  
11 user has the authorizations corresponding to the permissions data.

12  
13 In other aspects, the subsystem includes a communication section that  
14 engages an authorization server when the user does not have the requisite minimum  
15 authorizations of the permissions data set; or when a user desires to augment the  
16 permissions to a particular media by transacting a license to that media. The  
17 communication section thus includes a process section for transmitting transactional  
18 information to the server, and for receiving, from the server, auxiliary permission to  
19 utilize the media.

20  
21 The methods of the invention can include the steps of encrypting the media,  
22 and/or transferring the container to the data processor via one of point-to-point  
23 email, CD-ROM, ftp, gopher, smtp (email), and http (World Wide Web). In one  
24 aspect of the invention, for example, the registration server first authorizes a user  
25 with a PACKAGER through log-in process to establish a secure line, such as known  
26 in the art. The user and PACKAGER then generate the registration information  
27 relating to the particular CONTAINER, and transmit the information and a message  
28 digest to the registration server. Upon receipt, the registration server returns a  
29 "registration certificate," in digital form, that is signed by the server's private key.  
30 The registration server's public key is widely known, so that the registration server

1 can operate as a certification authority for the packaged-media. The registration  
2 certificate is then passed through secure channels, and the PACKAGER attaches the  
3 digital signature to the CONTAINER. Accordingly, authenticity is demonstrated to  
4 anyone with a VIEWER or PACKAGER that has access to the CONTAINER.

5  
6 In an alternative aspect, if the communication channel is unsecured, the  
7 registration certificate is encrypted via public key to the user's public key.

8  
9 These and other aspects and advantages of the invention are evident in the  
10 description which follows and in the accompanying drawings.

#### 11 12 Brief Description of the Drawings

13  
14 Figure 1 illustrates one system, constructed according to the invention, for  
15 managing copyrighted works formed as CONTAINERS;

16  
17 Figure 1A illustrates a schematic view of one CONTAINER constructed  
18 according to the invention;

19  
20 Figure 2 shows a schematic illustration of a VIEWER and SYSTEM  
21 EXTENSION subsystem, constructed according to the invention, and which is  
22 suitable for viewing selected information within a CONTAINER such as illustrated  
23 in Figure 1A;

24  
25 Figure 3 shows a schematic illustration of a PACKAGER system, constructed  
26 according to the invention, and which is suitable for encapsulating electronic media  
27 within a CONTAINER such as illustrated in Figure 1A;

1        Figure 4 illustrates a schematic diagram of a system which is constructed  
2        according to the invention and which provides for managing copyrighted electronic  
3        media assets;

4  
5        Figure 5 shows one illustrated use of the invention in the management of  
6        copyrighted GIF files;

7  
8        Figures 5a and 5b show illustrative dialog boxes displayed to a user of the  
9        system of Figure 5;

10  
11       Figure 6 shows a computer network constructed according to the invention and  
12       which illustrates selected operational uses of the invention;

13  
14       Figures 7-7h show illustrative computer displays for use with a system  
15       constructed according to the invention, such as the network of Figure 6;

16  
17       Figure 8 illustrates one acceptable process flow for providing copyright  
18       management according to the invention;

19  
20       Figure 9 schematically shows a system, constructed according to the invention,  
21       and which illustrates selective operations of a VIEWER, SYSTEM EXTENSION,  
22       PACKAGER and registration/authorization server;

23  
24       Figure 10 illustrates various components of the invention, including a  
25       CONTAINER, REGISTRY, OBJECT, SYSTEM EXTENSION, MATADATA, DIGITAL  
26       CREATIVE WORK, VIEWER, PACKAGER, TOOLBOX, DIGITAL CONTRACT; and  
27       further illustrates certain relationships between such components;

28

1        Figure 11 illustrates a system, constructed according to the invention, for  
2        managing digital creative works, and shows one operational interaction between a  
3        CONTAINER, REGISTRY, SYSTEM EXTENSION and TOOLBOX;

4  
5        Figure 12 schematically illustrates interaction between a  
6        PACKAGER/TOOLBOX, Registration Server, and SYSTEM EXTENSION, in accord  
7        with the invention;

8  
9        Figure 13 schematically illustrates one packaging process flow in accord with  
10       the invention;

11  
12       Figure 14 shows a representative property page template constructed according  
13       to the invention;

14  
15       Figure 15 illustrates a template overlaid onto an OBJECT that instantiates a  
16       CONTAINER constructed according to the invention; and

17  
18       Figure 16 schematically shows a registration server system constructed  
19       according to the invention.

20  
21       Detailed Description of the Invention

22  
23  
24       Figure 1 illustrates a system 10, constructed according to the invention,  
25       whereby CONTAINER 12a, 12b are created and packaged, and then registered on  
26       associated registration servers 14a, 14b, respectively. Users 16a, 16b and 16c are  
27       connected for data transfers with one or more of the authorization servers 18a, 18b,  
28       such as through a computer network or the Internet.

29  
30       The illustrated CONTAINERS 12a, and 12b are created as copyrighted media  
31       by author 19 and user 16a, a derivative author of the work 12a. For example, media

1 13 is representative of original work of authorship. Thereafter, the CONTAINERS  
2 12a, 12b are packaged as a data container, according to the systems and methods  
3 described herein, and as denoted by the copyrighted © symbol marked over the  
4 media. These packaged CONTAINERS 12a, 12b are registered on servers 14a, 14b,  
5 respectively, and are made available for license through authorization servers 18a,  
6 18b. A single server can operate as both the registration server and authorization  
7 server.

8  
9 In operation, the CONTAINERS 12a, 12b are available for limited free use  
10 according to the minimum permissions data set assigned to each CONTAINER.  
11 Typically, the minimum permissions allow users with access to the CONTAINER to  
12 view the CONTAINER, but not to save or otherwise transfer the CONTAINER  
13 without first obtaining auxiliary permission from the CONTAINER's authorization  
14 server. As illustrated, for example, users 16a, 16b each have access to CONTAINER  
15 12a and may therefore freely read or view the contents of the media within  
16 CONTAINER 12a at their associated personal computers 17a, 17b, respectively. If,  
17 however, the users 16a, 16b attempt to act on the CONTAINER 12a in a manner  
18 which is not in accordance with the permissions they hold, they are automatically  
19 prompted to obtain a license to the CONTAINER 12a. The licensing transaction  
20 occurs through the authorization server 18a, which connects and communicates with  
21 the users 16a, 16b through personal computers 17a, 17b. Alternatively, the users 16a,  
22 16b may, if desired, initiate a licensing transaction with the server 18a if they know,  
23 for example, that their permissions are insufficient to access the CONTAINER 12a in  
24 the desired way.

25  
26 Once licensed to the CONTAINER 12a, the licensed user has augmented  
27 auxiliary permissions to utilize the CONTAINER in some other way, such as saving  
28 and/or modifying the CONTAINER. Similarly, user 16c is connected via computer  
29 17c to the authorization server 18b, and may therefore view and, if desired, license

1 CONTAINER 12b through server 18b. The format of CONTAINERS 12a, 12b are  
2 described in more detail in connection with Figure 1A.

3  
4 CONTAINER 20 of Figure 1A provides a secure container for electronic  
5 media, including heterogeneous multimedia data types such as musical scores  
6 coupled with graphical images. More particularly, the CONTAINER 20 provides a  
7 package that encapsulates binary data objects, shown as the data container 23, and  
8 can contain some or all of the illustrated data components 21, 22, 24, 25 and 26.

9  
10 In Figure 1A, the Container Header 21 contains basic information about the  
11 CONTAINER 20, including, without limitation, information such as a unique file  
12 format identifier, a format revision code, a document creator application type, a file  
13 type (typically the MIME type code) of the enclosed data, a comment field length,  
14 and a comment field, typically up to about 256 characters. The information within  
15 Container Header 21 is generally not encrypted.

16  
17 The Container Identifier 22 uniquely identifies the CONTAINER 20 by the  
18 registration server upon which the CONTAINER has been registered, and the  
19 CONTAINER's registration or index number on that server. This registration code  
20 typically contains the server name and registration index. A registration server cross-  
21 reference table, working in conjunction with the Internet's Domain Name Service  
22 (DNS), is used to find the actual network address (typically a TCP/IP address) of the  
23 registration server. In one example, a unique server code may indicate local  
24 registration, usually indicating a work in progress. In another example, an author  
25 logged onto a computer, such as the author 20 of Figure 1, and actively generating a  
26 copyright work in progress, e.g., a novel in Microsoft Word™, will update and store  
27 the work on the local computer. In one embodiment of the invention, a work in  
28 progress is a locally accessible file which has not been authenticated through the  
29 registration process.

1       The Data Container 23 contains the information representing the electronic  
2 media or Digital Creative Work, typically in an original file format. If desired by the  
3 author, this data can be secured through encryption, such as through secret or public  
4 key methods known in the art. The data within the Container 23 is usually passed in  
5 the clear, i.e., unencrypted. However, increased control can be obtained through  
6 encryption of the associated media. The fields within the Data Container 23 can  
7 include the enclosed data file, and can include the data container extension code,  
8 and the data container size, among other information.

9  
10       The Source Works Extensions 24 provides a bibliographic record, or  
11 'persistence,' of copyright uses through generations of derivative work. The data  
12 fields within the Sources Works Extensions 24 can include any of the Source Works  
13 Extension Code, the Container ID, and the Permissions mask. If demanded by the  
14 licensor of the work, or desired by the licensee, the Container ID and the applicable  
15 permissions mask (the set of relevant use permissions) for the source work are  
16 included in the derivative work. In accord with the preferred use of the invention,  
17 the Source Works Extensions 24 are encrypted; and any number of Source Works  
18 Extensions 24 may be included in a CONTAINER 20. For example, information  
19 about successive derivative authors of the CONTAINER 20 are stored sequentially  
20 as a Source Works Extension 24. By way of another example, one Source Work  
21 Extension 24 can include the release information for any performer whose image or  
22 audio likeness appears in the current CONTAINER.

23  
24       The Source Works Extensions preferably operates to protect the source works  
25 author, even at the risk of burdening the derivative author and/or developer.  
26 Authors can require that their work is included as a source works extension in a  
27 derivative work, or they can leave this choice to the editor or derivative developer.  
28 Authors can also request that their source works are not displayed. For example,  
29 they may require the derivative developer to go through the authorization process  
30 again to obtain permissions and to include information regarding the work.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29

The Minimum Permissions 25 includes a permissions data set that are distributed with all authentic copies of the CONTAINER 20. These permissions affect the minimum use of the data within the Data Container 23 in cases where an on-line licensing transaction has not yet taken place. The Minimum Permissions 25 thus uphold the spirit of the fair use doctrine of copyrighted works; and the careful setting of the minimum permissions data set by the author(s) or creator(s) of the media ensures easy access and limited free use of the media up to the minimum authorized permissions set forth in the Minimum Permissions 20. This free use through minimum permissions is made possible by viewing the CONTAINER 20 through a SYSTEM EXTENSION, constructed according to the invention and described in more detail below, which is widely distributed to potential users of the CONTAINER 20.

Minimum permissions 25 are superseded by auxiliary permissions which are assigned to the CONTAINER 20 during an on-line licensing transaction. Auxiliary permissions are preferably contained in secure License Certificate documents provided by the Registration Server and encrypted to the licensee's key.

In accord with the preferred embodiment of the invention, an encrypted Digital Signature 26 is also part of the CONTAINER 20, to facilitate authentication. While the Signature 26 can be encrypted to ensure the authenticity and integrity of the CONTAINER 20, encryption of the bulk data 23 is also possible to guarantee a higher level of security.

Those skilled in the art will appreciate that other orderings of the information within the CONTAINER 20 are possible, including one where the Data Container 23 is last.

1        In accord with the preferred embodiment of the invention, users can  
2        unpackage or unwrap the CONTAINER 20 only through the controlled management  
3        of the copyrights associated with the CONTAINER 20. Specifically, the  
4        CONTAINER 20 is viewable through the SYSTEM EXTENSION and, if needed, a  
5        VIEWER. The VIEWER is available in several formats to accommodate the differing  
6        types of media contained within the CONTAINER. By way of example, once the  
7        CONTAINER 20 is recognized by the SYSTEM EXTENSION, documents formatted  
8        within the Data Container 23 of Figure 1A can be opened and manipulated on  
9        compatible applications such as:

- 10
- 11        • Stand-alone VIEWER applications, with SYSTEM EXTENSION functionality  
12        provided therein, which allow viewing of the media and of the networked  
13        licensing and registration information.
  - 14        • Applications which are fully OLE compliant and where the OLE2  
15        implementations of the SYSTEM EXTENSION, VIEWER and PACKAGER  
16        reside on the system.
  - 17        • Applications for which VIEWER and/or SYSTEM EXTENSION plug-ins may  
18        be available, so that user's of applications such as Adobe's Photoshop®,  
19        Premiere®, and Acrobat® can directly interface with CONTAINERS.
  - 20        • Applications with integrated kernel software encompassing VIEWER and  
21        EXTENSION-like functionality, such as for integration into World Wide Web  
22        software like Mosaic® and Netscape®.

23

24        The CONTAINER 20 of Figure 1A can also include information about the  
25        successive users of the CONTAINER. For example, the Source Works Extensions 24  
26        can have an appended data field or usage module which stores selected information  
27        about the users of the CONTAINER. Such usage information can include, for  
28        example, the identity and/or location of the user. Alternatively, the usage  
29        information can be stored at the associated authorization server during or in  
30        connection with a licensing transaction to the CONTAINER.

1  
2 In summary, the CONTAINER format of Figure 1A augments the  
3 multimedia data content with supplementary information which identifies, without  
4 limitation, some or all of the following information: the source, registry, and format  
5 of the data; the copyright legacy of the data; minimum permissions to use of the data  
6 prior to on-line licensing; a digital signature to prove authenticity of the data; and a  
7 use record of the users who accessed the media.

8  
9 Figure 2 illustrates a VIEWER and SYSTEM EXTENSION combination system  
10 30 constructed according to the invention and which is suitable for viewing the  
11 CONTAINER 20 illustrated in Figure 1A. The system 30 includes a series of process  
12 actuators 32a...32f, each of which decodes and/or interprets the several elements of  
13 the CONTAINER 20. The system 30 is connected for data transfer along data  
14 transfer line 34 to communicate and operate on the CONTAINER 36, stored for  
15 example on a server. The several process actuators 32 thereafter operate, in  
16 combination, to enable viewing of the media within the CONTAINER 36 and in  
17 accord with the minimum permissions data set. This media is illustrated in Figure 2  
18 as the data objects 38, which are, for example, displayed in a computer screen,  
19 through data transfer line 34a, so that a user can view the contents of the media data  
20 objects.

21  
22 The system 30 can be constructed as a printed circuit board, application  
23 specific integrated circuit, a VLSI circuit, or as a software module resident within a  
24 computer and operable in connection with an internal microprocessor to perform the  
25 various process actuator functions described below in connection with process  
26 actuators 32a...32f. Typically, the system 30 is connected for communication with a  
27 computer display so that once the CONTAINER 36 is unpackaged, the data objects  
28 38 within the CONTAINER 36 are viewable to the user.

1        More particularly, the process actuator 32a interprets selected information  
2 about the container header, e.g., the header 21 shown in Figure 1A. This information  
3 can, for example, include the type of file within the CONTAINER 36, or a comment  
4 field specifying certain details about the media as described by the media's author.  
5 Process actuator 32b, likewise, interprets selected information about the container  
6 identifier, e.g., the identifier 22 of Figure 1A. Such identifier information includes, at  
7 least, a unique identifier of the registration server upon which the CONTAINER 36  
8 is registered, so that appropriate on-line licensing transactions can occur with the  
9 appropriate location. Process actuator 32c interprets - and sometimes decrypts - the  
10 data formulating the media 38, so that the user can view the media 38 to evaluate  
11 whether to engage in a licensing transaction. The process actuator 32c provides  
12 minimum access to the media 38 in accord with the minimum permissions data set  
13 which is associated with the CONTAINER 36 and which is loaded and interpreted  
14 by the actuator 32d. Process actuator 32e interprets selected information about the  
15 source works extensions associated with the CONTAINER 36, while process  
16 actuator 32f interprets information about the digital signature associated with the  
17 CONTAINER 36, thereby providing a means to authenticate the media 38.

18  
19        Not all process actuators 32 are required in every system 30, depending upon  
20 the form of the CONTAINER 36. At a minimum, however, the system 30 must be  
21 able to interpret the data within the CONTAINER, including, if necessary, decrypt  
22 algorithms needed to unlock any encrypted data within the CONTAINER 36; and  
23 the system 30 must identify the CONTAINER's minimum permissions as well as the  
24 connectivity information of the CONTAINER's associated authorization or  
25 registration server. The system 30 will not, however, typically permit further  
26 actions - such as copying and/or downloading of the media 38 to disk - without first  
27 obtaining auxiliary licensing permissions from the associated authorization server,  
28 as described in more detail below. The system 30 thus provides a minimum access  
29 to the data 38, such as viewing the media contents on the user's display terminal,  
30 thereby promoting limited but fair use of the data 38.

1

2        Similarly, electronic media is packaged into a format such as the  
3 CONTAINER 20 through a packager system constructed according to the invention  
4 and denoted herein as a PACKAGER, such as illustrated in Figure 3. The  
5 PACKAGER system 40 of Figure 3 is suitable for generating the CONTAINER 20  
6 illustrated in Figure 1A. The PACKAGER 40 includes a series of process actuators  
7 42a...42f, each of which operates to formulate one or more of the elements of the  
8 CONTAINER 20, Figure 1A. The PACKAGER 40 is connected for data transfer  
9 along data transfer line 44 to communicate and operate on electronic media 46. The  
10 several process actuators 42 thereafter operate in combination to package or  
11 encapsulate the media 46 into a secure CONTAINER 48. For example, a user of the  
12 PACKAGER 40 is generally an author of copyrighted works, and one process  
13 actuator is used to specify the minimum authorized use of the media within the  
14 minimum permissions data set. The resulting packaged media, illustrated in Figure  
15 3 as the CONTAINER 48, is thereafter registered on a registration server, through  
16 data transfer line 44a, so that the CONTAINER 48 is available for on-line licensing  
17 transactions by any connected user having a SYSTEM EXTENSION and connected to  
18 the authorization server.

19

20        By way of example, the PACKAGER 40 can be constructed as a printed circuit  
21 board, an application specific integrated circuit, a VLSI circuit, or as software  
22 module resident within a computer and operable in connection with an internal  
23 microprocessor to perform the various process actuator functions described above in  
24 connection with process actuators 42a...42f. . Typically, the PACKAGER 40 is  
25 connected for communication with a registration server so that once the  
26 CONTAINER 48 is packaged, the data objects 46 within the CONTAINER 48 are  
27 available for license by any connected user.

28

29        Sufficient information is packaged within the document format to enable a  
30 potential licensee using the SYSTEM EXTENSION to engage in on-line licensing

1 transactions to obtain, for example, copyright ownership, licensing, and revenue  
2 information about the data. If the terms are acceptable, the potential licensee uses the  
3 SYSTEM EXTENSION to obtain additional permissions for derivative development  
4 or other use not covered in the minimum permissions data set. This operation is  
5 described below in connection with Figures 4-6.

6  
7 Figure 4 illustrates a copyright management system 50 constructed according  
8 to the invention. Specifically, Figure 4 illustrates how copyright permissions will be  
9 integrated into the multimedia production environment using the described  
10 CONTAINER format. The media is first formulated as individual content elements  
11 52 that are created and authored by media-specific tools, such as text editors,  
12 graphics tools, audio design tools, and digital video production tools. In the  
13 conventional production environment of the prior art, the elements 52 would simply  
14 enter a multimedia asset library, ready for use in production. No copyright  
15 information whatsoever would typically be affixed to the data objects prior to  
16 archiving.

17  
18 In system 50, on the other hand, content element-specific permissions are  
19 affixed to each data object 52 before passing on to the next level of production or on  
20 to archiving. In one embodiment of the invention, the system 50 incorporates a  
21 PACKAGER 54 within a stand-alone application to affix permissions and other  
22 related authorship information to the data 52, such as described in connection with  
23 Figure 3. Alternatively, the PACKAGER 54 can be directly integrated into the media-  
24 specific tools of the developers; and, as such, the PACKAGER 54 becomes a "plug-in"  
25 tool for commercially available graphics, video, and sound development  
26 applications based on the PACKAGER software kernel.

27  
28 After packaging by the PACKAGER 54, the heterogeneous content elements  
29 56 are registered on a registration server 58, and, for example, released to the  
30 production library. During this stage of production, a multimedia authoring or

1 scripting environment can be used to create an interactive multimedia program  
2 which is a composite of these archived elements 56. The control characteristics and  
3 asset utilization of the program embodied in the control "script" may also have an  
4 affixed permissions header. Thus all of the component assets will be protected in a  
5 similar fashion.

6  
7 For derivative uses of packaged CONTAINERS such as the packaged  
8 elements 60 of Figure 4, a VIEWER and PACKAGER 62 can be utilized as a plug-in  
9 to the associated application software which generated the media of CONTAINER  
10 60 in the first place, so that editing and saving of the CONTAINER can occur. Such  
11 modifications and saving correspond to a "derivative use," as described herein.  
12 Once the works 60 are modified and packaged into a derivative CONTAINER 64,  
13 including a Source Works Extension, they too are registered on a registration server  
14 58 (illustrated as a single server, for ease of illustration) for future licensing  
15 transactions, and, for example, released to a production library.

16  
17 The system 50 thus provides an effective strategy for managing both in-house  
18 and externally obtained copyrighted assets. In accord with one embodiment of the  
19 invention, a two-tiered rights clearing scheme is provided for multimedia program  
20 integration, in which both the encapsulated minimum permissions and the auxiliary  
21 permissions of all incorporated works are reverified prior to compilation. The  
22 specific content of this combination of permissions, including the permissions  
23 introduced by the creator of the composite work, will dictate what sort of  
24 authorization is required at execution time. Upon remote execution of the compiled  
25 multimedia program, a spectrum of authorization schemes are possible, from free  
26 execution, to the networked authorization of individual copyrighted assets. The  
27 licensing functionality of the PACKAGER/VIEWER kernel is applicable during  
28 execution as well as during production.

29

1 For illustrative purposes, Figure 5 shows a system 70, constructed according  
2 to the invention, which only manages copyrighted GIF (graphics files) media. The  
3 GIF CONTAINERS are created and/or modified through VIEWER and/or  
4 PACKAGER systems, such as described herein, and are managed through a  
5 registration server. Figure 5 shows, in particular, initial document processing, use-  
6 based licensing, header and extension maintenance, source work copyright  
7 clearance, local and remote server registration, and encrypted file formatting.  
8 Preferably, the system 70 is based on TCP/IP.

9  
10 The major functional sections of system 70 include opening files of  
11 appropriate types, creating and modifying headers and extensions, providing  
12 permissions clearance for included sources works and attached performance  
13 releases, and CONTAINER formatting, encryption, and saving. Each of these  
14 sections is described below:

15  
16 Opening Files

17  
18 CONTAINERS are loaded into the system 70 once packaged by a  
19 PACKAGER. For example, an original work 72 created in an application  
20 environment is opened in that environment and formatted by a PACKAGER into a  
21 CONTAINER 74. Alternatively, an existing CONTAINER 76 can be opened by a  
22 SYSTEM EXTENSION (and VIEWER if needed), modified if desired, and stored as a  
23 CONTAINER 74.

24  
25 More particularly, media is opened and available to the user through a  
26 combination of the application which created the media (i.e., the VIEWER) and a  
27 SYSTEM EXTENSION. In the case of raw GIF files, the images are displayed and a  
28 header editing dialog box appears to the creator, such as shown in Figure 5a,  
29 indicating that the system 70 is ready to start the formatting process. For  
30 CONTAINER-formatted files, a dialog box appears listing basic information for the

1 main file, such as shown in Figure 5b; and similar information is listed in a scrolling  
2 window for each of the Source Works.

3  
4 The CONTAINER's minimum permissions (obtainable and resident, for  
5 example, within any CONTAINER) and any auxiliary permissions (obtained from  
6 an authorization server during a licensing transaction) will dictate how the opened  
7 file may be used. To encourage browsing and fair use of CONTAINER-formatted  
8 works, the publicly distributed CONTAINER files will typically have sufficient  
9 minimum permissions to allow local viewing, at least, and sometimes unlimited  
10 local derivative use. Publicly-distributed files which allow local viewing can be  
11 opened by the SYSTEM EXTENSION (and VIEWER, if needed); and files which  
12 require licensing to be opened, or working files which have not yet been publicly  
13 registered, must be opened with the user's key.

14  
15 Publicly distributed files are registered on a registration server, and if  
16 encrypted, the key resident on the server is passed to the user via a secure channel.  
17 Some of these files will require licensing at viewing time, meaning that auxiliary  
18 permissions must be obtained. The auxiliary permissions files, or certificates, will be  
19 encrypted based upon the registered user's key, as are works-in-progress (not  
20 registered, and possibly with incomplete sources works clearance).

## 21 22 Creating & Modifying Headers & Extensions

23  
24 System 70 has several interfaces for creating or modifying the headers and  
25 extensions which embody the CONTAINER format. The Container Header, e.g., the  
26 header 21 of Figure 1A, is primarily derived from attributes of the enclosed media  
27 within the CONTAINER. These attributes are displayed in the DocInfo Editor and  
28 Viewer windows shown in Figure 5a. The Container ID, e.g., the ID 22 of Figure 1A,  
29 denotes the CONTAINER's registration server 78 and the index number of that  
30 CONTAINER on that server. Non-local document IDs can only be assigned if there

1 is a valid registration certificate associated with the file. Local Container IDs are  
2 encrypted, but can only be changed by the document owner. Container ID  
3 maintenance is typically handled through a computerized dialog box.

4

#### 5 Permissions Clearance and Source Works

6

7 For Source Works Extensions, e.g., the Extensions 24 of Figure 1A, the  
8 Container ID information is displayed in a scrolling view for the set of source works  
9 associated with the current file. A dialog box allows the CONTAINER IDs of  
10 additional works to be specified. Permissions information can be obtained by  
11 double-clicking an entry on this list. A transaction with the registration server 78 of  
12 the source works 72, 76 may be initiated by selecting the appropriate CONTAINER  
13 ID. Note that the user may choose to ignore clearances for locally-generated source  
14 works.

15

16 To enable permissions clearance for source works, public registration will not  
17 be permitted without proper source works clearance. This is ensured by the  
18 following: first, system 70 will not allow on-line registration to take place unless the  
19 permissions of the included source works (plus any auxiliary permissions) agree  
20 with the intended minimum permissions and maximum licensable permissions, the  
21 latter to be set at registration time. Secondly, the registration server 78 will not allow  
22 registration unless it is proven that the source works are clear. Clearances are  
23 required for those source works extensions with insufficient minimum permissions  
24 for the intended distribution of the derivative work. These clearances are in the form  
25 of auxiliary permissions, obtained on-line with licensing transactions identical to  
26 those discussed earlier. Given the intended minimum and licensed maximum  
27 permissions, the Source Works Manager Window displays those source works  
28 whose permissions need upgrading. The user will then select each one individually  
29 to launch a licensing transaction. Clearances that are encrypted are based on the  
30 user's key, and therefore cannot be transferred.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29

Private works, or works-in-progress, may not require registration, but any works which are to be publicly distributed — and, for example, encrypted using a secret key — must be registered. Users must therefore demonstrate that all source works in system 70 have been cleared prior to the registration attempt. Upon successful registration, the user of system 70 will receive an encrypted registration certificate which facilitates the saving of the CONTAINER in a publicly-viewable form. Since registration and authentication is based on a unique message digest for the file, if any changes are made to the file a new message digest must be calculated and the CONTAINER's entry in the registration-server database must be updated.

Encrypted data is preferably formatted with a secret key that is generated at the encryption event, and transported using public key encryption.

Applications compatible with system 70 are preferably based on TCP/IP, and therefore operate in the same manner as most popular Internet-compatible users.

Formatting, Encryption, & Saving

A PACKAGER of system 70 saves files in the CONTAINER format, such as described above, and preferably encrypts the data therein. Exemplary encryption schemes according to the invention include, without limitation:

- Encryption is initiated by the user, who also generates the secret key which is passed to the server, by secure means, and which becomes part of the registration record for that work. Upon the grant of auxiliary permissions, the server passes the key to the licensed user as part of the certificate. This is intended for publicly registered and distributed files, and a CONTAINER is not encrypted in this way without being registered first.

- 1       •       Encryption based on the author's key. All local works-in-progress may  
2       be encrypted in this way, ensuring that local use is possible but unregistered  
3       public use is not.
- 4       •       Encryption based on another user's key. This permits collaboration  
5       while protecting the collaborative work.

6  
7       With further reference to Figure 5, once a CONTAINER 74 is saved and  
8       registered on a server 78, it may be freely distributed. Derivative users 80 can gain  
9       clearance to the CONTAINER 78 through the SYSTEM EXTENSION (and VIEWER,  
10      if needed) and in accord with the minimum permission of the CONTAINER and the  
11      auxiliary permissions from servers of all source works. The work 82 represents  
12      either work in progress, or publicly available work; and can be encrypted, such as  
13      described herein.

14  
15      Figure 6 illustrates a computer network 90, constructed according to the  
16      invention, for managing copyrighted electronic media. In a first instance, an original  
17      author 92 generates and packages electronic media 93, e.g., such as described in  
18      connection with Figure 3, and registers the CONTAINER 93 on registration server  
19      94. Typically, the author 92 generates the work 93 on a computer that is connected to  
20      the network via data transfer line 96. Once the author 92 registers the CONTAINER  
21      93, the server 94 becomes an authorization server for any subsequent access and/or  
22      licensing of the CONTAINER 93.

23  
24      By way of example, user 96 has a VIEWER and is connected to the network 90  
25      through communication line 97. The user 96 can thereby access the CONTAINER 93  
26      through the authorization server 94 up to the minimum permissions data set forth in  
27      the CONTAINER format. Typically, the minimum permissions permit viewing of  
28      the CONTAINER; but do not permit saving and/or transmission of the  
29      CONTAINER. Should the user so desire, he or she can license the CONTAINER  
30      through an on-line licensing transaction with the authorization server 94 to obtain

1 additional authorizations - denoted herein as auxiliary permissions - to use the  
2 media within the CONTAINER for some other use, e.g., saving or modifying the  
3 CONTAINER.

4  
5 Similarly, a Derivative User/ Author 100 of the CONTAINER can access and  
6 modify the contents of the CONTAINER by first obtaining auxiliary permissions to  
7 do so through the authorization server 94. More particularly, the author 100 first  
8 views the CONTAINER via the SYSTEM EXTENSION (not shown) and VIEWER  
9 and through the minimum permissions data set of the CONTAINER; then transacts  
10 a license with the Authorization server 94 to obtain the auxiliary permissions. The  
11 author 100 is thus connected via data transfer line 102 to the server 94; and has a  
12 SYSTEM EXTENSION, VIEWER and PACKAGER resident at his computer (note, for  
13 illustrative purposes, the Users and Authors 96, 100 and 120 of Figure 6 are shown  
14 with limited detail; and generally include a computer with SYSTEM EXTENSIONS,  
15 VIEWERs and/or PACKAGERs resident at the computer).

16  
17 Once the derivative user 100 modifies the CONTAINER, the CONTAINER is  
18 registered on registration server 104, through data transfer line 103, so that  
19 subsequent licensing can occur by users such as user 110. Note that user 110 must  
20 obtain licensing authorization from each server 104 and 94. This process is done  
21 automatically at the user's computer terminal. The user 120 first accesses the  
22 modified CONTAINER through the network 90 and by connection with the server  
23 104 through data transfer line 105. Once the user 110 views the modified  
24 CONTAINER, she can seek auxiliary permissions to use the data for her intended  
25 use. Such auxiliary permissions are obtained by connecting to each of the servers 94  
26 and 104 through data transfer lines 107 and 105, respectively.

27  
28 Derivative author 112, connected to the server 104 via data transfer line 114,  
29 operates a VIEWER and PACKAGER (and, if desired, a SYSTEM EXTENSION) in an  
30 SDK environment. Briefly, the SDK indicates a "Software Development Kit" and

1 enables developers of advanced multimedia applications, games, or multimedia  
2 authoring tools (including content creation applications) to incorporate System  
3 Extension, Viewer and Packager functionality into their applications in advanced  
4 ways. The SDK is appropriate, for example, when conventional OLE 2.0 compliance  
5 does not deliver the functionality or performance that the ISV demands. As above,  
6 the author 112 edits and creates multimedia works and packages them through the  
7 PACKAGER resident in the SDK to provide for registration and subsequent  
8 licensing of that work.

9  
10 To maintain the authorship of, and ownership to a CONTAINER within the  
11 network 90, sourceworks extensions are used. This extension can be resident within  
12 the CONTAINER, such as shown in Figure 1A, so that the appropriate CONTAINER  
13 authorship and/or ownership is recorded and stored in the appropriate data  
14 element within the CONTAINER. Alternatively, or concurrently, the sourceworks  
15 extension is stored on any and all of the servers 94 and 104. In this way, the owner or  
16 authors of the CONTAINER can ensure persistence through generations of  
17 derivative use. Further, use information can also be stored within the sourceworks  
18 extension, so that, for example, an owner of the server 94 or 104 can independently  
19 track the use of his or her copyrighted works simply by downloading the  
20 information at the server 94 or 104.

21  
22 In general, each of the servers 94, 104 are owned and operated independently  
23 from the other. By way of example, one typical owner of the server 94 is a  
24 multimedia house which generates copyrighted works for sale and distribution.  
25 Such an owner thus seeks to restrict access to the media to authorized users, thereby  
26 protecting the copyright.

27  
28 Each of the servers 94, 104 also provides selected use-base information about  
29 the CONTAINERS registered and licensed through the servers. Specifically, the  
30 selected use-base information provides a way to assess charges to the owners of the

1 servers for services rendered in connection with the servers 94, 104. The use-base  
2 information is available by physically accessing the server 94, 104; but is more  
3 conveniently obtained by phoning the server and downloading the information  
4 directly. This information is not available for general users; but is typically available  
5 only to the administrator who set up the servers 94, 104 in the first place. This  
6 administrator can, for example, receives fees from the respective owners of the  
7 servers 94, 104 as part of this arrangement.

8  
9 For example, such an administrator would make revenue for several  
10 transactions and sales shown in Figure 6, including: (A) registrations of  
11 CONTAINERS on both registration servers 94, 104; (B) one licensing transaction for  
12 auxiliary permissions for user 96; (C) two licensing transactions for auxiliary  
13 permissions for user 110; (D) two PACKAGER modules resident at the computers of  
14 Author 92 and Derivative Author 100; (E) two registration modules to configure the  
15 servers 92, 104; and (F) one SDK module resident at author 112 (typically, the SDK  
16 includes a SYSTEM EXTENSION, VIEWER and PACKAGER).

17  
18 Those skilled in the art should appreciate that Figure 6 is illustrative only, and  
19 that many other configurations of a computer network are possible within the scope  
20 of the invention. For example, the network 90 can include a multitude of registration  
21 and authorization servers; and any connected computer which has the SYSTEM  
22 EXTENSION (and VIEWER, if needed) can access media on the network up to the  
23 minimum permissions authorized by the minimum permissions data set within the  
24 CONTAINER housing the respective media.

25  
26 The sections below provide more detail about the invention, and include  
27 descriptive and operational commentary of the SYSTEM EXTENSION, VIEWER,  
28 sourceworks information, User Registration & Certification, the PACKAGER, SDKs,  
29 registration servers, and authorization servers, among others.

30

## VIEWERs and SYSTEM EXTENSIONs

In conjunction with the SYSTEM EXTENSION, the VIEWER allows viewing and editing of graphic, image, video, audio, and textual objects that are packaged into a CONTAINER in accord with the invention. Where objects are individually packaged, viewing and editing will be done within the window of the source application or designated viewer. Where objects are content elements within a compound document, in-place viewing and editing will be common, with an external window session being optional. Data objects - i.e., media - that are packaged according to the invention can be dragged and dropped, for example, between OLE 2.0-compliant applications such that all attribute information contained in the CONTAINER remains intact during such an operation.

The SYSTEM EXTENSION is required for viewing and editing any CONTAINER. The PACKAGER and TOOLBOX are complementary to the SYSTEM EXTENSION and one is required to package media within a CONTAINER, e.g., the CONTAINER 20 of Figure 1A. Typically the PACKAGER or TOOLBOX is required to create derivative works from a CONTAINER; but only the SYSTEM EXTENSION is required by developers when the minimum permissions of the source works do not require clearance. This might be common for so-called "public domain" free use of works.

The SYSTEM EXTENSION examines certain attribute information encapsulated with the data object in compliance with the CONTAINER format. Operations on the data object from within the VIEWER or editor are restricted based on the minimum permissions encapsulated with the data object and any Auxiliary Permissions subsequently obtained for the data object. By way of example, the "Container Info" window of Figure 7 provides a local summary of the document, including all available minimum and auxiliary permissions.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30

The SYSTEM EXTENSION also facilitates on-line licensing of CONTAINER-packaged works. Based on registration information encapsulated with the data, i.e., the Container ID, the SYSTEM EXTENSION contacts the CONTAINER's Registration Server and initiates an authorization transaction. After the user is authenticated (typically utilizing the user's RSA digital signature, whereby the user's key is stamped by a certification authority), the user uses a template-like interface to request auxiliary permissions, such as shown in Figure 7a. If the permissions request does not match the user's requirements, the request may be edited, such as shown in Figure 7b. Based on the available Transaction Rules in the database for the user's classification, licensing terms are presented to the user, such as shown in Figure 7c. If the terms are accepted, a digital certificate is issued containing the auxiliary permissions for that specific derivative use and encrypted to that specific user.

The License Request window, such as shown in Figure 7a, is the entry point for licensing transactions. The Registration Server is identified and the set of requested permissions is displayed. If the User recently attempted an unauthorized operation, the permissions displayed are those required by that operation. The user has the option to edit the request, such as shown in Figure 7b, to proceed with the transaction, or to cancel out. When the user has submitted the Request, a License Agreement, exemplified in Figure 7c, is returned to a display terminal of the requesting user. This interface, such as shown in Figure 7c, allows the user to verify the terms of the agreement and to agree to those terms.

The SYSTEM EXTENSION can be used to obtain extensive information about the authorship, ownership, and licensing terms of a creative work prior to any licensing transaction. This information may be a combination of data permanently encapsulated with the object, including for example authorship and basic document information, and information stored on the registration server, including for example copyright ownership, licensing terms, royalty schedules, and other

1 augmented document Information. Figure 7d illustrates the typical information  
2 which is available from the Registration Server and which can be displayed in a  
3 Registry Info window.

#### 4 5 Source Works Information

6  
7 The SYSTEM EXTENSION can also be used to obtain source works  
8 information for the media object. The Sources Works Display, for example and as  
9 shown in Figure 7e, presents the electronic record of any work from which the  
10 current work is derived, and the available information about each of those works.

#### 11 12 User Registration & Certification

13  
14 A user who wishes to engage in an on-line transaction with a REGISTRY  
15 typically presents an RSA-based, network-standard digital signature signed by a  
16 recognized Certification Authority. Accordingly, SYSTEM EXTENSIONS and  
17 PACKAGERS can contain RSA-based standardized procedures for creating and  
18 managing public/private key pairs, for engaging in certification transactions, and  
19 for becoming registered users. The Certification Authorities require human  
20 intervention when authenticating an individual's personal information. When valid  
21 information is received, the individual's key is stamped with a unique code from the  
22 Certification Authority which recognizes its authenticity. This certification is  
23 apparent before anything is encrypted to that key, and is apparent when the key is  
24 used to verify a digital signature (which can only have been signed by the individual  
25 using the matching key).

#### 26 27 PACKAGER

28  
29 The PACKAGER is used by authors and publishers to encapsulate  
30 authorship, ownership, minimum use permissions, and source works information  
31 with a creative work and in a secure package. During this encapsulation, the original

1 binary file format of the creative work is preserved. An object created by the  
2 PACKAGER can stand alone, or can be incorporated in a compound multimedia  
3 CONTAINER. The PACKAGER is required for any editing sessions which involve  
4 CONTAINER-packaged works and which demand clearance for derivative use.

5  
6 During an editing session, the PACKAGER maintains a list of all  
7 CONTAINER-packaged source works, their minimum permissions, and any  
8 auxiliary permissions which have been granted to the current work in progress. The  
9 Source Works Manager window, such as shown in Figure 7f, allows the developer to  
10 easily see the status of permissions for each work, to obtain detailed authorship,  
11 ownership, and licensing information from the source work's registration server, and  
12 to selectively obtain auxiliary permissions as required for each source work.

13  
14 For example, the user can command the display of all CONTAINER-  
15 packaged source works from the Source Works Manager window of Figure 7f. For  
16 each individual source work, the user may review the minimum permissions and, if  
17 available, any auxiliary permissions which have been issued. If the user chooses to  
18 obtain auxiliary permissions or to upgrade the current set displayed, a licensing  
19 transaction is initiated with the source-work's registration server.

20  
21 Alternately, the PACKAGER can prompt the user to upgrade the permissions.  
22 This happen during the registration process in the following way: after preparing the  
23 CONTAINER data for the derivative work, including the requisite minimum  
24 permissions, the user executes a Check Clearance, wherein all accumulated  
25 permissions are checked against the minimum permissions which the developer  
26 intends to encapsulate with the derivative work. All sourceworks with permissions  
27 that are insufficient will be listed in the Clearance Status window.

28  
29 The Check Clearances function is also applied to the set of Transaction Rules  
30 which the developer intends to load on the Registration Server. The basic principle is

1 that a derivative work may not grant more rights to the use of a source work than  
2 what was available before the derivative work was created.

3  
4 Some of the CONTAINER information which is encapsulated with the data  
5 object by the PACKAGER is prepared from context automatically. Other information  
6 can or should be manually entered or selected by the user through the a dialog  
7 window such as the DocInfo Editor Window of Figure 7g, such as:

8  
9 (1) Revision Number: The revision number identifies a version of the  
10 document format which the PACKAGER complies with.

11  
12 (2) Data Format and Creator Application: This provides the type of data  
13 contained within the CONTAINER, and the application environment which  
14 created the CONTAINER. Note, however, that these fields may have reduced  
15 functionality when used, for example, with OpenDoc and OLE 2.0. In such a  
16 case, the DocInfo Editor can display the information, but it does not need to  
17 be contained as a separate DocInfo field if the Object CONTAINER can be  
18 interrogated for it.

19  
20 (3) Minimum Permissions: As described above, the minimum  
21 permissions template provides a way for the user to generate the minimum  
22 permissions that are encapsulated in the CONTAINER. One acceptable set of  
23 permissions, such as shown in connection with the Minimum Permissions  
24 Editor window of Figure 7h, includes:

- 25  
26 • Opening/Viewing restricted  
27 • Modifications restricted  
28 • Drag & Drop restricted  
29 • Printing restricted  
30 • Format Changes restricted  
31 • Saves restricted  
32 • Registration of derivative works required  
33 • Store Source Works Extensions on Registration Server

- Require Source Works Extensions
- Restrict Source Works Extensions

(4) Source Works Extensions: The identification of source works extensions is managed by the Source Works Manager, described, in part, in connection with Figure 7f. The author of the works can also track unregistered or non-CONTAINER-packaged source works using the Source Works Manager, which allows authorship and ownership information to be textually entered into the Registration Server's database when the derivative work is registered. When information or authorization is requested, only contact information will be provided.

(5) Digital Signature: The Digital Signature provides authenticity and integrity of all information contained in the CONTAINER. One secure way to do this is to attach a RSA digital signature to the CONTAINER, which is provided by the registration server upon license. The author is a registered user in this case, and the CONTAINER is registered on a Registration Server. Appropriate evidence of certification and the CONTAINER's hash results are contained in the signature.

The PACKAGER can also enable encryption of the media within a CONTAINER. If an author chooses to encrypt the media, a random key for the media is generated; and during a secure registration transaction with the registration server - such as after a log-on and once the author proves she is authorized to use the server - the secret key is passed by either (i) a secure communication channel, or (ii) a certificate that is public-key encrypted to the user's key, so that only that user may use that issuance of the secret key. This encryption method provides for strong security since secret keys are randomly generated and are unique to a CONTAINER; and the distribution of the key to the CONTAINER is handled by the server.

1        Those skilled in the art will appreciate that other encryption methods are  
2 suitable for use with the invention and without departing from the scope of the  
3 invention.

#### 4 5 6    SDKs

7  
8        As discussed above, the Software Development Kit (the SDK) enables  
9 developers of advanced multimedia applications, games, or multimedia authoring  
10 tools (including content creation applications) to incorporate SYSTEM EXTENSION,  
11 VIEWER and PACKAGER functionality into their applications in advanced ways.  
12 The SDK is appropriate, for example, when conventional OLE 2.0 compliance does  
13 not deliver the functionality or performance that the ISV demands.

14  
15        The SYSTEM EXTENSIONS, VIEWERs and PACKAGERs of the invention  
16 operate with most OLE 2.0-compliant content creation tools and with most tools that  
17 create compound works. The SDK permits the developers to follow their own  
18 coding standards but still take advantage of the invention.

#### 19 20    Registration Server

21  
22        The Registration Server of the invention contains the set of services used by  
23 information creators who want users of their works to be able to easily identify  
24 ownership, obtain licensing terms, and license those works on-line. The  
25 Authorization Server module is the set of services those information users (who may  
26 also be information creators) will use to obtain access to information and license  
27 those works. The Server maintains a database of registry information pertaining to  
28 creative works which rights-holders are making available for commerce.

29  
30        The process of initiating a database entry for a work is called Registration.  
31 The act of processing a user's request for augmented permissions is called

1 Authorization or licensing. Before starting a transaction with the Server, the  
2 PACKAGER does the following:

3

4 • Verify that the user is a registered user. It will look for the user's RSA key  
5 with a certification stamp from an approved certification authority.  
6 Preferably, user registration capabilities are built into all VIEWERs and  
7 PACKAGERs.

8

9 • Ensure that the user completes the Transaction Rule Templates, used in  
10 designing the licensing rules for all available classes of users. This should  
11 be completed prior to contacting the Server because they determine  
12 whether sufficient clearances have been obtained.

13

14 • Ensures that the user completes the Ownership Information Template,  
15 which is the textual information that a user of the work would receive  
16 when using the VIEWER to obtain further ownership information, beyond  
17 what might be encapsulated in that package.

18

19 • Verifies that sufficient clearances (auxiliary permissions) for all source  
20 works used in the current work-in-progress are available to the  
21 PACKAGER.

22

23 • If the clearances are insufficient, the PACKAGER guides the user through  
24 the series of authorization transactions required to get the necessary  
25 permissions.

26

27 • When sourceworks clearances are complete, the PACKAGER performs a  
28 one-way hash function contained, for example, in an RSA Digital  
29 Signature and which become part of the works' database record for later  
30 authentication.

- 1
- 2       • As a last step, the PACKAGER contacts the Server.
- 3

4       The PACKAGER testifies to the Server that the user is authentic and that all  
5 sourceworks (if any) used in the work being registered have been properly cleared.  
6 The Server then assigns a unique registration ID to the CONTAINER (based, for  
7 example, on the server's ID and the number of documents registered on the server)  
8 and builds the database record based on the information held by the PACKAGER.

9

10       In "signing" the CONTAINER, the PACKAGER preferably assembles a RSA  
11 Digital Signature for the package. Contained within the signature are the  
12 registration ID and the results of the one-way hash on the document data. The  
13 signature is encrypted to the User's key, thus demonstrating authenticity.

14

#### 15   Authorization Server Module

16  
17

18       Before starting a licensing transaction with the Authorization Server, the  
19 SYSTEM EXTENSION does the following:

- 20       • Determines that available permissions (minimum and auxiliary) are not  
21 sufficient to perform the user's desired action.
- 22       • Verifies that the user is a registered, which is required only if a transaction  
23 with the Server is necessary.
- 24       • Testifies that the user is registered and presents the authorization request  
25 (a request for specific auxiliary permissions) to the Authorization Server.  
26 The user's classification is also transferred and stamped with certification  
27 from the associated Certification Authority.
- 28

1           Based on the requested auxiliary permissions and the classification of the  
2 user, the Server presents its terms for licensing. These terms are viewable within a  
3 display window and can include, without limitation, any of:

- 4
- 5           • Actual permissions granted
- 6           • Payment options. When a choice of on-line payment methods are  
7 available, a provider-specific window becomes available after the method  
8 is chosen. When some other method is required, an appropriate window  
9 to facilitate the payment is displayed.
- 10          • Request human intervention. The user or the Server may not be satisfied  
11 with an on-line authorization request. In that case, the option exists to  
12 pursue some form of human intervention. The options which the  
13 registering party has made available are displayed.
- 14          • Accept terms. When the licensing terms are accepted, a packet  
15 enabling the auxiliary permissions is transferred to the user's computer.  
16 These are encrypted to the user and thus are non-transferable.

17

18           The systems and methods of the invention encompass novel methods and  
19 tools which will enable creators of networked multimedia programs to identify their  
20 media and to claim their rights. This is enabled, in part, by bundling the copyright  
21 information with the data element, and by formatting the CONTAINER in a manner  
22 which maintains this identification and attribution so that it persists with the  
23 copyrighted work through generations of derivative use. The invention therefore  
24 demonstrates the application of copyright permissions to a hierarchy of network-  
25 distributed data objects to effectively protect owners' rights.

26

27           This invention also facilitates the licensing of multimedia content by different  
28 classes of users. In accord with the invention, a desktop tool can be integrated with  
29 selected viewing or production tools to feature an interactive licensing template. The  
30 invention thus demonstrates the integrated support of hierarchical permissions

1 headers in the production environment, and demonstrates networked interactive  
2 licensing within the production environment based on hierarchical permissions.

3  
4 Figure 8 illustrates one acceptable process flow for managing copyrighted  
5 works in accord with the invention and corresponding to the methods and systems  
6 described herein.

7  
8 Figure 9 illustrates a system 200 constructed according to the invention. The  
9 system 200 includes a server 202 which operates as a registration and authorization  
10 server for any of the CONTAINERS 204a, 204b, 204c, and 204d stored in a library  
11 206. By way of example, the library 206 can be a publisher's library of any or all of  
12 the original works owned by or authored for the publisher. Author 208, for example,  
13 illustrates one such author connected to the library 206 through a personal computer  
14 210 and communication line 212. The computer 210 is a data processor that includes  
15 a PACKAGER 214 constructed according to the invention and as described  
16 hereinabove. In the preferred embodiment, the PACKAGER 214 is a software  
17 module stored within the computer's internal memory 210a to control the data  
18 processor's actions in accord with the invention. Through the PACKAGER 214, the  
19 author 208 can create and package any of the CONTAINERS 204. The computer 210  
20 also includes a communication section 210b, to facilitate on-line communications,  
21 and a computer display 210c.

22  
23 The CONTAINERS 204 are secure containers of electronic media, as described  
24 herein, and are stored in the library 206 as digital files, such as within a CD-ROM, or  
25 within a computer memory. Preferably, the CONTAINERS are stored such that a  
26 user such as User 216 can access the CONTAINERS through an on-line connection  
27 218 between the user's personal computer 220 and the library 206.

28  
29 The owner of the library 206 may also have copyrights in CONTAINERS such  
30 as CONTAINER 204e, which represents a CD-ROM of a media-packaged work that

1 is distributed to the User 216 by mail. The CD-ROM 204e, for example, exemplifies  
2 one other published work that is created by the author 208 and packaged by the  
3 PACKAGER 214. As above, the server 202 also functions as the registration and  
4 authorization server for CONTAINER 204e.

5  
6 In accord with the invention, the user's computer 220 is a data processor that  
7 includes a SYSTEM EXTENSION 222 constructed according to the invention and as  
8 described hereinabove. In the preferred embodiment, the SYSTEM EXTENSION 222  
9 is a software module stored within the computer's internal memory 220a to control  
10 the data processor's actions in accord with the invention. A CD-ROM 224 drive is  
11 preferably connected to the user's computer 220 via data line 220d to facilitate access  
12 to CD-ROM files such as CONTAINER 204e.

13  
14 Through the SYSTEM EXTENSION 222 (and a VIEWER, if needed), User 216  
15 can access any of the CONTAINERS 204a-e up to the minimum permissions  
16 authorized by each of the CONTAINERS. By way of example, the minimum  
17 permissions data set within each CONTAINER typically authorizes the User 216 to  
18 view the CONTAINERS 204a-e; but not to download, modify, save or otherwise  
19 electronically transfer the CONTAINERS. The data transfers required to access the  
20 CONTAINERS 204a-d up to the minimum permissions data set occur through  
21 communication line 218; while the only data transfers required to access the  
22 CONTAINER 204e up to its minimum permissions data set are between the  
23 computer 220 and the CD-ROM drive 224.

24  
25 If the User 216 wishes to augment the authorizations to any of the  
26 CONTAINERS 204, for example to modify or save the CONTAINER at the computer  
27 220, she must communicate with the server 202 and transact a license with that  
28 server. The data processor 220 thus includes a communication section 220b that is  
29 connected for data transfers, over communication line 226, with a compatible  
30 communication section 202a of the server 202. Upon selection by the User 216, the

1 VIEWER 222 determines from the selected CONTAINER 204 that authorization  
2 server 202 is assigned to handle all licenses to that CONTAINER, and the SYSTEM  
3 EXTENSION controls the computer 220 to connect to the server 202 at the right  
4 address so that an on-line licensing transaction can occur.

5  
6 Specifically, once the user 216 indicates that additional permissions to the  
7 CONTAINER 204 are desired, the SYSTEM EXTENSION can display selected terms  
8 to the CONTAINER, as stored within the CONTAINER or as stored within the  
9 server 202. In either case, the SYSTEM EXTENSION causes the computer 220 to  
10 generate a licensing request signal and issue that signal to the server 202. Preferably,  
11 the user 216 also designates - through the SYSTEM EXTENSION - the desired use of  
12 the media within the CONTAINER. The user 216 can thereafter accept the licensing  
13 terms to the CONTAINER 204, and, if accepted, the user 216 receives notification  
14 from the server 202 that auxiliary permissions are granted for the desired use.

15  
16 In the event that CONTAINER 204 is a derivative work, the SYSTEM  
17 EXTENSION 222 determines that auxiliary permissions are also required, for  
18 example, from server 228, the server designated by the original author of the media  
19 within CONTAINER 204.

20  
21 The server 202 stores transactional information about the CONTAINERS 204.  
22 For example, each license transacted through the server 202 is stored in a file 229a,  
23 such as within a computer memory 230. In this way, the owner or administrator of  
24 the CONTAINERS can assess the licensing fees generated by the CONTAINERS.  
25 Likewise, the server 202 also stores information or files 229b that set forth the  
26 number of CONTAINERS registered thereon, so that, again, the owner or  
27 CONTAINER-administrator can assess server usage. The files 229a, 229b are  
28 preferably available through the communication section 202a.

1           In one embodiment of the invention, the server 202 includes an internal  
2 memory 202b, connected to the communication section 202a, that stores selected  
3 information about the CONTAINERs registered thereon. For example, licensing  
4 terms to the CONTAINER 204 can be stored within the memory 202b. A relay  
5 section 202c operates to relay such terms to the processor 220 in response to a license  
6 request signal prompted by the user 216. A data comparison section 220d operates to  
7 compare the user's reply to the licensing terms, and to generate and transmit the  
8 requested auxiliary permissions when the response signals correspond to the  
9 requisite terms specified in the license information stored in memory 202b (or  
10 alternatively in the CONTAINER). Accordingly, once the user 216 receives the  
11 auxiliary permissions, that user is provided with additional authorizations to use the  
12 media within the CONTAINER 204; and the SYSTEM EXTENSION 222 enables the  
13 user 216 to access the CONTAINER 204 up to the maximums allowed in the  
14 bumped-up permissions data set.

15  
16           Figure 10 illustrates a system 298, constructed according to the invention, and  
17 provides a brief description of several components of the invention; and further  
18 illustrates certain relationships between such components. First, the system 298  
19 provides for the making and manipulation of CONTAINERs 300 and 301. As  
20 illustrated, a CONTAINER such as CONTAINER 300 can occupy a single block of  
21 memory such within memory 302 (e.g., memory 302 can be solid state RAM within  
22 a computer 304, or ROM memory within a web server 304). Each CONTAINER has  
23 one or more Digital Creative Works and Metadata. The CONTAINER 300, for  
24 example, has DIGITAL CREATIVE WORK 306 and associated METADATA 308.  
25 The WORK 306 is the electronic expression created, for example, by an author or  
26 publisher, and is shown as a letter "Z" for clarity of illustration. The METADATA  
27 308 provides selected information about the WORK 306; and such information can  
28 include, for example, the author's name, the minimum permissions or minimum  
29 authorized uses of the WORK 306, and licensing details.

30

1       A CONTAINER can also occupy a plurality of locations on the Internet 307.  
2       This is illustrated by CONTAINER 301, which has several parts 301a, 301b and 301c  
3       linked through the Internet 307. As illustrated, for example, the CONTAINER 301  
4       includes DIGITAL CREATIVE WORK 310a and 310b, each at a different location  
5       312a, 312b, respectively; and METADATA 314b and 314c, each at a different location  
6       312b and 312c, respectively. For illustrative purposes, location 312c is here shown as  
7       a REGISTRY 316 that serves as the registration server for CONTAINER 301.

8  
9       The computer 318 illustrates one of a number of users of the Internet 307. As  
10      such, computer 318 typically houses web browser software 320, such as Internet  
11      Explorer™, within internal memory 322. The computer 318 also has communication  
12      software and hardware 326 which facilitates communication with the Internet 307.

13  
14      Other software is also present within the computer 318. Within the operating  
15      system memory 328, there resides a SYSTEM EXTENSION 330 which recognizes  
16      and which enables interaction with CONTAINERS such as CONTAINERS 300, 301.  
17      By way of example, a user at computer 318 can surf the WWW (i.e., the Internet 307)  
18      and locate the CONTAINER 301 at web server 304. The CONTAINER 301 can be, for  
19      example, displayed on a web page at the user's screen 332 as OBJECT "Z" that  
20      instantiates the CONTAINER 301. In the event the computer 318 does not have the  
21      EXTENSION 330 installed thereon, the CONTAINER 301 can include, within the  
22      METADATA 308, a location on the WWW 307 to find and obtain such a SYSTEM  
23      EXTENSION 330. One location, for example, can be an administrative web site 334  
24      that is also connected to the WWW 307 with a unique web address. When  
25      requested, the site 334 downloads the EXTENSION 330 to the computer 318 so that  
26      the computer 318 can render the OBJECT "Z". Since the OBJECT "Z" is generally a  
27      graphic or text, e.g., a JPEG or Microsoft Word™ document, that was formed by a  
28      third party application software, then the computer 318 should further house, for  
29      example, a "VIEWER" 336 such as a JPEG viewer or the Microsoft Word™  
30      application.

1  
2 In operation, a user thus sees the OBJECT "Z" which instantiates the  
3 CONTAINER 300. Normally, the user at computer 318 will not notice anything  
4 different about the OBJECT "Z" as compared to any other graphic or visual within a  
5 web page. However, when the user clicks on the OBJECT "Z" by operation of the  
6 mouse 318a, then that user will be given additional information, such as the  
7 associated METADATA 308. Further, if the user at computer 318 attempts an  
8 operation - e.g., copying into another file or printing on the printer 318b - that is  
9 prohibited according to the instructions in the METADATA 308, then that user will  
10 be so notified and informed that a license is needed to accomplish that action.

11  
12 By way of example, suppose the CONTAINER 300 is registered at the  
13 REGISTRY 338, which is a registration server for the CONTAINER 300. When the  
14 user at computer 318 is notified of an improper operation, the user will be given the  
15 opportunity to obtain a license to the Digital Creative Work 306 through interaction  
16 with the REGISTRY 338. The METADATA 308 specifies that registration server 338  
17 is designated with this role; and further specifies the REGISTRY address so that the  
18 computer 318 can locate the REGISTRY 338 on the WWW 307.

19  
20 Figure 10 also illustrates a second computer 340 that represents an author or  
21 publisher of Digital Creative Works. As such, the invention provides a way to  
22 package the Work with a CONTAINER. For example, computer 340 includes a  
23 PACKAGER or TOOLBOX 342 which packages Digital Creative Work such as the  
24 work 344 on the screen 340c, here illustrated as the letter "Y". Typically, the Work  
25 344 is made by a third party application, e.g., Adobe Photoshop™. As such, the  
26 computer 340 typically includes this software within internal memory. In Figure 10,  
27 this software is referred to as VIEWER 346 because the application is typically the  
28 same application that is later required to view or utilize the Work 344.

1       Once the user at computer 340 packages the Work 344 within a CONTAINER  
2 348, the Work 344 will have attribution for any location on the web 307. As such, the  
3 user at computer 340 can send the CONTAINER 348 onto the Internet 307 for  
4 storage, if desired, at a web site or at a REGISTRY such as REGISTRY 338. When  
5 other users, e.g., a user at computer 318 locate and access the CONTAINER 348,  
6 such a user sees the OBJECT "Y" as the instantiation of the CONTAINER 348. If the  
7 user attempts an operation that is prohibited, then the CONTAINER 348, through its  
8 Metadata, locates and phones its home, which in this example is the REGISTRY 338,  
9 to begin a licensing transaction.

10  
11       Figure 11 illustrates a system 400 constructed according to the invention.  
12 Figure 400 further illustrates general and preferred operations and functionality of  
13 the system 400 in the management of Digital Creative Works. In Figure 11, user  
14 stations 402 and 404 are computers for users of digital media connected to the  
15 Internet 406 and to each other via a network or Intranet 408. User stations 402 and  
16 404 are connected to the Internet, and to the Intranet 408, via local data lines 402b  
17 and 404b, respectively.

18  
19       User stations 410 and 412 are used by creators or authors of Digital Creative  
20 Works 410a, 412a, respectively; and are connected to the Internet 406 by data lines  
21 410b and 412b, respectively. Digital Creative Work 410a is shown illustratively as an  
22 "A" on the screen 410c of user station 410; while Digital Creative Work 412a is  
23 illustratively shown as an "A+B" on screen 412c of user station 412. The Work 412a  
24 is denoted as "A+B" to indicate that the Work 412a is a combination of creative  
25 works of both authors at stations 410 and 412.

26  
27       Those skilled in the art should appreciate that each of the stations 402, 404,  
28 410 and 412 have hardware (not shown) which enables communication with the  
29 Internet 408 and/or Intranet 406. For example, such hardware often includes a  
30 modem and supporting software to facilitate communication through the Internet

1 408, to other users, such as through email, and to selected web sites, FTP sites, URLs,  
2 newsgroups, databases, and the like.

3  
4 User station 410 also has a TOOLBOX 414; and user station 412 has a  
5 PACKAGER 416. The TOOLBOX 414 and/or PACKAGER 416 are used to create a  
6 CONTAINERS, here illustrated as CONTAINERS 418 and 420. CONTAINER 418  
7 derives from the work 410a of station 410; while CONTAINER 420 derives from the  
8 work 410a and the work 412a of station 412. CONTAINERS 418 and 420 are shown  
9 connected to the data lines 410b, 412b to illustrate that the CONTAINERS are  
10 transmitted through, or dispersed on, the Internet 408.

11  
12 Each of the user stations 402, 404, 410 and 412 has a SYSTEM EXTENSION  
13 422 installed into an associated internal memory 402d, 404d, 410d and 412d,  
14 respectively. These EXTENSIONS 422 operate with the operating system of the  
15 associated station so as to recognize, interact with, and access CONTAINERS.

16  
17 User stations 402 and 404 additionally have VIEWERS 424 installed into  
18 internal memory 402d and 404d, respectively. The VIEWERS 424 are used to view  
19 and interact with the Works within CONTAINERS. By way of example, if an  
20 OBJECT 410a is a graphic that is best viewed with a JPEG VIEWER, then the  
21 EXTENSION 422 calls that VIEWER to render the OBJECT 410a as needed to the  
22 user 402. Note that user 402 sees the OBJECT "A" as the instantiation of the  
23 CONTAINER 410. Likewise, user 404 sees the OBJECT "A+B" as the instantiation of  
24 the CONTAINER 420.

25  
26 The Registry 426 operates to register selected CONTAINERS, and to negotiate  
27 as agent for any author of a CONTAINER. Preferably, the Registry 426 has internal  
28 memory 426d which can be used to store CONTAINERS, METADATA to  
29 CONTAINERS, or parts of CONTAINERS and/or METADATA. It is important to  
30 note that a CONTAINER need not reside at a single memory location. Those skilled

1 in the art will appreciate that a CONTAINER based on object technology can be, and  
2 is intended to be, dispersed across the Internet 408 so that different portions of the  
3 CONTAINER reside at the most logical location for that portion.

4  
5 For illustration purposes, Figure 11 also shows an administrative site 428 (and  
6 associated Registry 428a), which can operate to augment the system 400, as  
7 described below; and a generic web site 430 that provides database information such  
8 as commonly provided on the WWW. As above, those skilled in the art should  
9 appreciate that the administration site 428 and web site 430 include associated  
10 hardware (not shown) to facilitate the needed communication with the Internet 408  
11 and other users 402, 404, 410 and 412 of data therein.

12  
13 In operation, the system 400 has many features, some of which are illustrated  
14 in Figure 10. Specifically, work 410a is instantiated on the screen 410a as OBJECT  
15 "A." By way of example, "A" can represent a digital representation of a drawing or  
16 sketch by the author. By way of further examples, "A" can be made electronically,  
17 such as through a graphic artist program (using the keyboard 410f and mouse 410g)  
18 such as Adobe Illustrator™; or "A" can be hand-drawn and scanned within the  
19 computer 410 by an optical scanner, such as known to those skilled in the art.

20  
21 In one example, the author of CONTAINER 418 makes the Digital Work "A"  
22 for enjoyment only; and does not choose to register the CONTAINER 418 with the  
23 REGISTRY 426. However, the author at station 410 does desire recognition as the  
24 author of the work "A," so he encapsulates METADATA 418b within the  
25 CONTAINER 418 that specifies his name. User 410 thereafter sends the  
26 CONTAINER 418 onto the Internet 406, where it is stored as a web page at the  
27 database or web-site 430.

28  
29 Other users, connected to the Internet 408 and web-site 430, who have a  
30 SYSTEM EXTENSION resident at their computer, can access the OBJECT "A" of

1 CONTAINER 418. By clicking on the OBJECT A, or through such other authorized  
2 action as specified by the author 410, such a user can additionally obtain information  
3 about the author's name in the METADATA 418a.  
4

5 By way of example, the user at user station 402 is interrogating the Internet  
6 408 through visual interaction with her display 402c of the WWW (note for clarity of  
7 illustration that no accompanying mouse and keyboard are illustrated with user  
8 stations 402 and 404; and even though they are not required, it is intended that such  
9 instruments are present). User 402 accordingly has web browser software 432 (e.g.,  
10 Netscape™ and Microsoft Internet Explorer™) installed in internal memory 402d on  
11 the computer 402. When the user at station 402 encounters the web page with the  
12 CONTAINER 418, typically seen as OBJECT A referring to the CONTAINER 418, the  
13 SYSTEM EXTENSION 422 and VIEWER 424 permit viewing of the OBJECT "A." The  
14 author's name can also be displayed, if desired, through the METADATA and as  
15 specified by the author at station 410.  
16

17 Note, again, that because the CONTAINER 418 is integrated with object  
18 controls utilizing ActiveX™, or similar object control, the CONTAINER 418 need not  
19 comprise data that is resident at the same location. Rather, a CONTAINER can  
20 include data that is spread across the network 406 or Internet 408. Because the  
21 CONTAINER 418 is formed with object-based controls, when user station 402  
22 encounters the web page at site 430 that refers to the CONTAINER 418, the  
23 computer 402 first interrogates its registry to see if that control is available internally.  
24 If not, the computer automatically finds and installs the control over the Internet 408  
25 based upon the address specified by the author at station 410.  
26

27 The user at station 412 represents an author and a user of CONTAINERS. In  
28 particular, user station 412 has a SYSTEM EXTENSION 422 within internal memory  
29 412d so that it can access the CONTAINER 418 at web site 430. In this example, the  
30 user at station 412 chooses to edit the CONTAINER 418 through use of the

1 PACKAGER 416, also resident in memory 412d, so that the CONTAINER 420  
2 contains both digital creative works 412a and METADATA as selected by the user at  
3 station 412. The work 412a is illustratively shown as "A+B" in Figure 1.

4  
5 Accordingly, the work 412a created at station 412 is "derivative" in nature,  
6 since it derives from previous artistic work (i.e., the work 410a) of the author at  
7 station 410. The invention keeps track of the derivative uses and edits of digital  
8 creative works in a source works file disposed within the METADATA, as described  
9 herein.

10  
11 In this example, the user at station 412 chooses to register the work 412a with  
12 the Registry 426. Accordingly, the user at station 412 first initiates a registration  
13 request to communicate and request registration of CONTAINER 420. Depending on  
14 the type of work 412a, the user at station 412 can select a corresponding property  
15 page template to identify and select certain METADATA as associated with the  
16 CONTAINER 420. By way of example, any of the following information can be - or  
17 are required to be - communicated to the Registry 426, depending upon how the  
18 particular Registry is set up:

- 19
- 20 • The author's name and other rights related information (attributes or  
21 properties) of the work 412a.
  - 22 • The aesthetic presentation of the attached information (METADATA)  
23 for the work 412a.
  - 24 • The balance between accessibility and locality of the CONTAINER's  
25 properties. For example, certain static METADATA, such as the author's  
26 name, can be located in the CONTAINER 420; whereas requests for volatile  
27 METADATA information, such as quantity of works 412a to be published, is  
28 generally referred to a remote server. For example, the web site 430 or station  
29 412 can each function as such a remote server; and the author at station 412

1 can specify, or change, the number of published quantities of the work 412a as  
2 needed.

3 • The minimum permissions, auxiliary permissions and requirements for  
4 use of the work 412a by any user.

5 • The specification of other services, such as email, that are available  
6 through access to the CONTAINER 420.

7 • The sets of attributes, presentations, and permissions that are applied  
8 to the multiple works 410a and 412a.

9 • The specification of prototypes or templates of sets of attributes,  
10 presentations, and permissions that are formally and legally appropriate to  
11 the works 410a and 412a.

12 • The organization of attribution and credit to the work 410a, since the  
13 work 412a is a derivative work.

14 • The REGISTRY can have multiple templates available for different  
15 business models, different media types, and different categories of registrants.

16 • The subsequent processing by Registry 426 in evaluating, granting, and  
17 tracking permitted uses of the work 412a.

18 • Structure to comply with the protocols established by various  
19 registries. Note that although a single Registry 426 is illustrated in Figure 1,  
20 multiple registries are possible and intended. For example, had the user at  
21 station 410 registered the work 410a at a Registry other than Registry 426,  
22 then that Registry would require certain protocols and information (e.g.,  
23 addresses) to identify that Registry and to communicate thereto.

24  
25 This example is not a common occurrence whereby the original creator, user  
26 410, chose to make an unregistered OBJECT "A". Such a creator 410 thus preferably  
27 makes the unregistered OBJECT A with "open" permissions so that the associated  
28 Work 410a can be incorporated into other works, e.g., the Work 412a. Once the  
29 derivative user 412 uses the Work 410a, then the identification of the original author,  
30 i.e., "source work", will be reflected in the source works page of the new template, if

1 available. The onus is on the user to contact the creator by whatever means that  
2 creator lists in the property pages of the unregistered OBJECT A, possibly a phone,  
3 fax, email, or other contact. As such, an unregistered OBJECT can carry substantially  
4 all the information of a registered object.

5  
6 The users at stations 410 and 412 can thus package CONTAINERS from  
7 within creativity tools, within an Application Programming Interface (API) for a  
8 particular plug-in, or directly from the shell: in the case of the user at station 410, the  
9 TOOLBOX 414 indicates that the work 410a was created from within a creativity tool  
10 such as Adobe Illustrator™; while station 412 has a PACKAGER 416 installed as a  
11 direct shell application to produce CONTAINERS. These tools, together with the  
12 registration process at the Registry 426, assure the user that the attached  
13 METADATA information is not easily removed, altered or forged. Such users are  
14 then able to catalog, share, and generally manipulate such sets in an organized way;  
15 and with a large degree of automated help from the system 400. The attached  
16 METADATA information is accessible from any representation of the works 410a  
17 and 412a, especially from a rendition of the content as well as any iconic ones.

18

19 User station 404 is very similar to the user station 402, except that the user at  
20 station 404 has accessed a registered work 412a, as opposed to the unregistered work  
21 410a in CONTAINER 418. Accordingly, the METADATA 420b of CONTAINER 420  
22 specifies the minimum permissions of the work 412a. Typically, for example, that  
23 minimum permissions allows the user 404 to view the work 412a on the screen 404c;  
24 yet further actions such as print, copy, drag and drop are prohibited and are not  
25 possible without a license to the work 412a. By way of example, if the user at user  
26 station 404 desires to print fifty copies of the work 412a, then a license to this activity  
27 must be negotiated through the Registry 426, where the CONTAINER 420 was  
28 registered. If the METADATA 420b permits the license of the work 412a in terms of  
29 the number of prints, then the user at station 404 can contact the Registry 426 and  
30 proceed with appropriate licensing terms.

1  
2       Once created, CONTAINERS live on as data items within the Internet 408. It is  
3 likely that the individual or company which created the work associated with a  
4 particular work no longer exists relative to the Internet 408 and Registry 426. For  
5 example, one creator of Digital Creative Works is a publisher of magazines; and if  
6 that magazine goes out of business, then subsequent licenses to their works are  
7 problematic. There are several ways to deal with this problem. First, the publisher in  
8 such a situation can notify the Registry that it is going out of business and that future  
9 transactions as to their CONTAINERS are prohibited. Alternatively, the publisher  
10 can inform change the METADATA within the CONTAINER so as to unregister the  
11 CONTAINER, thereby providing a free license to the works within the  
12 CONTAINER. Note that the publisher could specify, in the METADATA,  
13 information about the publisher and suggestions for alternative contact points; and  
14 that METADATA is available to users with VIEWERS.

15  
16       In a default situation, where the publisher does nothing relative to its  
17 orphaned CONTAINERS, the Registry 426 can contact the administrative site 428 to  
18 decide the fate of the CONTAINER. At that point, the administrative site can specify  
19 that no additional information is known; and, for example, that access to the  
20 CONTAINER is prohibited.

21  
22       The administration site 428 also operates in default situations where the  
23 Registry does not answer. In that case, the administration site 428 can review the  
24 status of the CONTAINER and inform the requesting user to call the Registry later,  
25 for example if a temporary problem exists or if the Registry is too busy.  
26 Alternatively, the administrative site can function as an alternative Registry, if set up  
27 by the creator of the CONTAINER.

28  
29       The invention thus supports commerce between the owners and creators of  
30 digital content, i.e., the Digital Creative Work. Specifically, the invention provides a

1 method for the owner to license the work, while also providing a method for the  
2 multimedia developers and publishers to make productive use of the work's  
3 content. The invention thus provides a uniform, timely, and persistent means of  
4 identifying digital content in the networked environment.

5  
6 In a preferred embodiment of the invention, an Internet-based application is  
7 built around the OBJECT as supported by the TOOLBOX and the Registration  
8 Server. The SYSTEM EXTENSION enables OBJECTS to be viewed on target  
9 operating systems and from within a variety of applications. Preferably, the  
10 invention incorporates object technology such as Internet-extended OLE, the  
11 standard object technology developed by Microsoft™ that allows a variety of media  
12 types to be shared by applications throughout the Internet. One such interaction,  
13 according to the invention, is illustrated in Figure 12.

14  
15 The invention also provides substantially uniform representation of content  
16 within other applications. That is, creativity tools such as graphics, sound, video,  
17 word processing, and multimedia authoring tools are presented with a substantially  
18 uniform interface to host applications, relieving those applications from the  
19 responsibility of rendering all media types. Further, the creators and owners of  
20 content (i.e., Digital Creative Works) can, with the invention, store and make  
21 available the METADATA which can be critical to licensing and other derivative  
22 uses.

23  
24 The invention creates documents, or CONTAINERS, through a process called  
25 packaging. The PACKAGER merges content (i.e., Digital Creative Work), Metadata,  
26 and active interface controls and presents this to the user through a set of property  
27 pages designed for the specific business problem being addressed. The result of this  
28 packaging is instantiated as an OBJECT. Figure 13 illustrates one packaging process  
29 according to the invention. In Figure 13, Digital Creative Work and Metadata  
30 associated with that content are combined with the desired template to create the

1 OBJECT.

2

3 For an owner or creator, a CONTAINER is much easier to track and to  
4 manage than conventional content because the Metadata is accessible directly from  
5 the CONTAINER. Typically, the owner or creator will choose to attach a small  
6 amount of identifying data to the Digital Creative Work, with the larger and/or  
7 most volatile data being supplied to the CONTAINER from a remote registration  
8 server via the Internet. After the work is packaged as a CONTAINER, owners and  
9 creators can ensure that potential users always obtain up-to-date ownership, contact,  
10 and licensing information about specific content elements. Owners can thus be sure  
11 that the positive identification, direct communications, and possibility of automated  
12 licensing will maximize the likelihood that their content will get used in legitimate  
13 or legal derivative works.

14

15 CONTAINERS also reduce the workload of multimedia developers,  
16 publishers, and other derivative users of content by making the identification of  
17 content and its ownership substantially instantaneous and by reducing or  
18 eliminating delays, errors and misdirection when communicating with the  
19 appropriate rights management authorities.

20

21 In accord with the invention, one way to convert Digital Creative Works to  
22 CONTAINERS and OBJECTs begins with the use of a Template Editor. The  
23 Template Editor presents an interface for designing sets of properties and property  
24 pages that organize the presentation of the CONTAINER's Metadata and buttons  
25 that initiate various functions of the OBJECT. Specifically, the Template Editor  
26 enables content owners to create layouts for property pages, placing various controls  
27 on the pages. These controls can, without limitation, include:

28

- 29
- 30 • Fields for static data that will ultimately be bound to the object
  - 31 • Fields for dynamic data that will ultimately be stored on a remote server
  - Labels for clarifying or identifying sections of the property page

- Buttons for initiating an email or web access action
- Buttons for retrieving dynamic data from a remote server
- Other elements including illustrations, logos, or icons

One illustrative property page template is shown in Figure 14. Another template and an associated OBJECT, instantiating a CONTAINER, is shown, representatively, in Figure 15.

After creating the property page template, a user of the invention can employ one of several tools to make the CONTAINER: the Toolbox, the Express Packager, and the Software Developers Kit (SDK). Each tool merges the various input elements to create a CONTAINER or Object. In one illustrative case, the user of the tool specifies the source content element (e.g., photo, sound, video, text, etc.) and the Template to be used in the packaging process. The user then supplies the data required by the Template. Once all the data is supplied, the PACKAGER, taking its basic instructions from the Template, creates the CONTAINER, binding static data to the content and automatically storing dynamic data on the designated Registration Server. The various PACKAGER tools are designed for different applications and needs:

- In one configuration, the TOOLBOX is a graphical desktop tool designed for individual users packaging relatively small amounts of content. From a standard graphical user interface, the user specifies the content source file and designates the appropriate Template. The Toolbox then prompts the user for the necessary input to complete the required entries specified by the Template. Upon completion of the required entries, the Toolbox will update the associated server with dynamic data, if any, and create a CONTAINER.
- The Express Packager is a batch-oriented PACKAGER tool which converts high volume content elements to CONTAINERS. When using the Express Packager, the operator specifies a set of content files, the template, and a source of the required input data. The Express Packager then automatically accepts the input and converts the files to the right format.

- The SDK Packager is designed for applications where functionality according to the invention is to be built into existing content production tools. As an example, certain Internet publishers provide various "just-in-time" content delivery systems. In such a case, the SDK Packager is used whereby the publisher's existing production tools automatically invoke the packaging process to follow the same model of receiving content, template, and data as input to produce the CONTAINER.

In the process of packaging, an owner can create a registered object by communicating with the Registration Server. Alternatively, the owner can use one of the packaging tools to create an unregistered object. In such a case, static information is bound to the content but there is no record placed on a Registration Server.

The Registration Server provides the communications link to Objects. Usually, it is the creator of the Template who establishes the relationships between the dynamic data required by the Object and the Registration Server. The Registration Server listens for various types of requests entered by viewers of the content (i.e., the Digital Creative Work). Those requests can be for specific elements of data that will be displayed on property pages, or for other data that will support functions such as email or web site addressing. The requests may also include transactions that require interfacing to legacy business systems or financial transaction systems.

The Registration Server is built to respond to such requests and to interface with existing information and transaction systems. In such a role, it can:

- Retrieve product information or pricing from a vendor's remote database and supply it so it can be displayed on a property page.
- Retrieve content ownership, contact, and licensing information from a publisher's remote database.
- Receive an incoming payment request and submit it to a third-party payment

1 handling system.

- 2 • Supply transaction activity data to an in-house marketing database.

3  
4 Many institutional content owners with existing business information and  
5 transaction systems can choose to have those systems interoperate with, or as, the  
6 Registration Server. Other users, however, can opt for an Administration Server.  
7 The Administration Server is a database that contains document and business  
8 information and transaction rules pertaining to owner's distributed content. The  
9 Administration Server is used to supply this information to the Registration Server  
10 when requested by the a user interacting with an OBJECT.

11  
12 Viewing OBJECTs, accessing property pages, and initiating other operations  
13 discussed above, according to the invention, requires SYSTEM EXTENSION  
14 functionality. Specifically, the SYSTEM EXTENSION acts as an extension to the  
15 user's operating system, ensuring that required functionality is available from  
16 within various applications and not just through an Internet browser. The SYSTEM  
17 EXTENSION is preferably compact, self-installing, and freely distributed via the  
18 Internet or as part of a customer's packaged solution.

19  
20 As discussed above, the CONTAINER can be created by the Toolbox or  
21 Express Packager. In creating the CONTAINER, the content owner, either by way of  
22 the Toolbox or the Express Packager, associates Digital Creative Work with  
23 Metadata, such as artistic or business attribution information (credits) and  
24 permission parameters. It is intended that the invention operate with all standard  
25 digital formats for the underlying source work, including GIF, JPEG, WAV, AVI,  
26 and others. In one embodiment of the invention, the content owners edit the  
27 Metadata values or properties using a set of Property Pages as an interface. The set  
28 of required and optional properties for a particular OBJECT are defined by a  
29 Template, created using the Template Editor. The Template also describes the visual  
30 layout used in the property page presentation of the Metadata. A variety of

1 Templates may be created and applied to different types of content and for different  
2 business or licensing models.

3  
4 A content owner can also choose to create either registered or unregistered  
5 CONTAINERS. In the case of unregistered OBJECTs, all content and Metadata  
6 properties are stored in the CONTAINER itself. In the case of registered objects, the  
7 Metadata properties are typically stored in two locations: within the CONTAINER  
8 and remotely on a Registration Server. Properties stored within the CONTAINER  
9 are referred to herein as static; properties that are retrieved from a Registration  
10 Server are referred to herein as dynamic, since their values may change during the  
11 life of the CONTAINER.

12  
13 If the CONTAINER is to be registered, a Template supplied by the designated  
14 Registration Server is used. That Template specifies the dynamic properties to be  
15 supplied by the user that will be transferred to and stored in the Registration Server.  
16 If an unregistered object is to be created, the content owner can select one of several  
17 default Templates or he can create a custom Template that allows static attribution  
18 information and communications with the creator/owner by email and web page  
19 access only.

20  
21 Registered CONTAINERS are better suited to content that is destined for  
22 commercial use. Advantages of registration include authentication, ability to serve to  
23 the user variable data such as terms for licensing, ability to change information after  
24 distributing the object, and automated transactions. Unregistered CONTAINERS  
25 may be desirable for material with a very short life cycle (e.g., weather maps), very  
26 low value (e.g., vacation photos), or for non-commercial distribution where the user  
27 simply wants to attach identifying information and facilitate email or web page  
28 access.

29  
30 The following are a few of the major features of CONTAINERS and OBJECTs,

1 as created by the invention:

- 2 • Viewing and Access - Objects can be rendered on systems where SYSTEM  
3 EXTENSION functionality is installed.
- 4 • Restrictions - CONTAINERS encourage compliance with the Copyright Laws  
5 by intercepting attempts to perform certain types of operations on the Digital  
6 Creative Work (e.g., drag-and-drop, copy, save or print).
- 7 • Content - The CONTAINERS can contain all standard and commonly used  
8 formats for image, sound, video, and text display.
- 9 • Property Pages - Property pages adhere to standard representations  
10 consistent with the operating system and other applications. Static data is  
11 displayed on pages. Also, for Registered Objects, dynamic data can be retrieved  
12 on demand from a Registration Server.
- 13 • Other security measures, described above, can be used to ensure the integrity  
14 of the CONTAINERS, preventing unauthorized and undetected modifications to  
15 the content or METADATA.
- 16 • CONTAINERS provide the capability to initiate communications to a  
17 creator/owner through the following mechanisms:
  - 18 – Email - Email addresses can be stored in the CONTAINER's properties,  
19 and email messages can be initiated when viewing the Object's property  
20 pages. Email messages can be edited and transmitted a number of ways  
21 including SMTP (direct Internet mail protocol), MAPI (Mail API) or by  
22 launching a user's configured email client application (e.g., Eudora or  
23 Microsoft Exchange).
  - 24 – Web page access - URLs can be stored in the CONTAINER's properties,  
25 and a web browser such as Netscape Navigator™ or Microsoft Internet  
26 Explorer™ can be launched to access the specified page.
  - 27 – Registration Server transactions - Registered CONTAINERS can initiate a  
28 variety of transactions with a Registration Server. Transactions include the  
29 retrieval of Dynamic Properties, the completion of a Permission Contract,

1           and payment for licensing fees. These transactions can be authenticated  
2           using cryptographic techniques.

3  
4           SYSTEM EXTENSION functionality provides the necessary functions to allow  
5 a user to render an OBJECT and to access property pages and functions. It is  
6 generally provided (e.g., "delivered") as an extension to the operating system. The  
7 SYSTEM EXTENSION is intended to be widely and freely distributed online and  
8 through traditional distribution media such as CD-ROMs and diskettes. Such  
9 extensions should have the following properties:

- 10 • Compact - The Extensions will often be loaded electronically by a user through a  
11 web-page or FTP server.
- 12 • Self-installing - The Extension can be installed with little or no interaction.
- 13 • Self-updating - Updates required for subsequent releases will be automatically  
14 detected and installed.
- 15 • Backward Compatible - New Versions of the Extension will always be able to  
16 view and use older OBJECTS.
- 17 • Forward Compatible - Objects with new formats and capabilities, created with  
18 newer versions of the Toolbox and Express Packager, can be viewed with older  
19 versions of the System Extension. The older System Extension can, for example,  
20 ignore new features or functionality supported by the newer Objects. This is  
21 analogous to viewing web pages using newer HTML extensions (e.g., tables or  
22 frames) with older browsers.

23  
24           The Registration Server is the storage and administrative facility for  
25 registered CONTAINERS. A registration server is the primary component required  
26 for organizations running a REGISTRY. A REGISTRY is, for example, analogous to a  
27 Web site, except that instead of sending HTML pages and responding to requests  
28 with the HTTP protocol, the REGISTRY is interacting across a network with  
29 OBJECTS. A REGISTRY can include a batch or real-time link to an organization's  
30 legacy permission or rights management system. The major functions of the

- 1 Registration Server can, without limitation, include:
- 2 • Object Registration - The Registration Server is the where the dynamic properties  
3 for a registered CONTAINERS are stored. These properties can be updated by  
4 the Registration Server administrator when necessary. Objects retrieving these  
5 properties will immediately reflect the updated values.
  - 6 • Template Creation - The Template Editor provides the operator of a registration  
7 server with the ability to create and customize Templates, including the layout of  
8 property pages and the definition of the static and dynamic properties to be  
9 associated with Objects. Templates can be organized and grouped for  
10 distribution to creators/owners for use with the Toolbox or the Express  
11 Packager.
  - 12 • Creator/Owner Registration - Several options are available for initiating a  
13 relationship with a creator/owner depending upon the business model adopted  
14 by the operator of a registration server. These options range from assigning a  
15 simple user account name and password to a sophisticated high-security  
16 procedure using officially certified digital signatures.
  - 17 • External System Linkages - The Registration Server can interface to existing  
18 rights management systems through one of several mechanisms:
    - 19 – The Express Packager allows one-way batch creation of Objects.
    - 20 – The Packaging API allows real-time creation of Objects. The API is two-  
21 way, enabling the update of data in the external system based on changes  
22 made to the Registration Server.
    - 23 – The Registration Server Database Mapper allows a direct interface from  
24 the Server to an existing external database. The Mapper allows a flexible  
25 mapping of the Object Properties to legacy systems.
  - 26 • The Report Writer - Pre-formatted and customized reports are available,  
27 including the following classes of reports:
    - 28 – Registered Object Reports
    - 29 – Creator/Owner Account Reports
    - 30 – Inquiry and Permission Transaction Reports

- 1           - Server Activity Reports
- 2           - Systems Operation Reports

3  
4   One exemplary Registration Server schematic is shown in Figure 16.

5  
6           The Registration Server also provides for certain problem situations that may  
7   arise with Objects.

- 8   • Servicing Objects for which the Registration Server record has been removed or  
9   transferred. If ownership has been transferred, then a transaction request may  
10   simply be redirected to the appropriate server. A special "backstop" server can  
11   be provided so that an Object contact the backstop server if all other attempts to  
12   locate the appropriate Registration Server fail. This server includes a master  
13   directory of Registration Servers. If the relationship between the creator and the  
14   Registration Server has terminated, then an appropriate notification will be  
15   returned.
- 16   • Servicing Objects which submit requests that for one reason or another violate an  
17   authenticity check. If the server receives any unusual transaction requests,  
18   including requests indicating an authentication failure, then an audit trail will be  
19   maintained.

20  
21           The Administration Server is an add-on component for operators of the  
22   Registration Server. The Administration Server, for example, serves small  
23   publishers, service bureaus, and independent professionals who do not have existing  
24   methods for administering royalties, handling on-line financial transactions, and  
25   reporting on the financial and administrative activity of the system. The  
26   Administration Server brings some of the necessary publishing functionality to the  
27   small user.

28  
29           As discussed above, the packaging process associates Metadata with Digital  
30   Creative Works and instantiates the CONTAINER as an Object. In one method of the  
31   invention, the METADATA is displayed by means of its property pages; the

1 properties required on these pages and their layout is specified by the object's  
2 property page template. Templates can be used for both registered and unregistered  
3 Objects, but are of special importance when an OBJECT is registered.

4  
5 The Template Editor enables the operator of a Registration Server to create  
6 and customize templates, including the layout of property pages and the definition  
7 of the static and dynamic properties to be associated with Objects. Templates may be  
8 organized and grouped for distribution to creators and owners for use with the  
9 Toolbox or the Express Packager. The Template Editor preferably has a GUI with a  
10 palette-oriented desktop motif consistent with current visual software design tools  
11 (e.g.: Visual Basic).

12  
13 A Template contains a hierarchy of data items, including, without limitation,  
14 the following:

- 15 • A collection of property pages.
- 16 • For each property page, a collection of controls that will appear on that page.
- 17 • For each property page, a collection of property sets. A property set is a collection  
18 of property descriptors that define the attributes of each property.
- 19 • The definition of the template's home Registration Server.
- 20 • The definition of the template's connection object.

21  
22 The Template Editor gives the user the tools to define property sets and their  
23 associated property descriptors. Each descriptor is uniquely identified upon  
24 creation. Each property page interface is built from a set of controls. The user selects  
25 each control from a palette and draws on a form in a fashion similar to Visual Basic.  
26 For each control selected, the user can define a new property descriptor to be  
27 associated with the control or may select from a set of "hard-coded" routines that the  
28 selected control can execute. Each control is assigned a unique identifier upon  
29 creation.

30

1       After the user has created property pages and property sets, the user can save  
2 everything as a Template that can be inserted into another Template Editor project.  
3 Alternatively they may save the work as a bound template that can be used directly  
4 by a packaging tool to create Objects. Prior to saving the user's work as a bound  
5 Template, the Template Editor automatically generates an input data form that may  
6 be optionally edited. When saving as a bound template, the template editor  
7 generates a fixed-format input data file that will be parsed by the PACKAGER.

8  
9       The Express Packager is used by content owners who convert large amounts  
10 of content into CONTAINERS by automatically merging Metadata and Digital  
11 Creative Work. The Express Packager creates registered and unregistered Objects  
12 and generally has two modes of operation:

- 13     • Conversion Mode enables large numbers of existing digital files to be converted  
14       into CONTAINERS. When operating in conversion mode, the Express Packager  
15       actively gets the content and the input data file that describes the Metadata and  
16       creates the CONTAINER. Data is either retrieved from a database or from a text  
17       file or other intermediate container storing the pertinent information.
- 18     • Creation Mode enables the Express Packager to operate under the control of  
19       another program through the real-time Packaging API (LPAPI). In this way, the  
20       Express Packager operates in a passive mode, taking its instructions from other  
21       applications. This mode is appropriate for packaging content that is created in  
22       real-time such as the output from Java applications, CGI scripts, proprietary  
23       publishing applications, etc.

24  
25       The LPAPI can be made available through an OLE Automation interface to  
26 enable a flexible and industry-standard protocol used to create and register Objects.  
27 The LPAPI allows custom interactive or batch interfaces to be built using a large  
28 array of development and scripting tools such as Visual Basic, C++, Microsoft Office  
29 applications, and other similar applications.

1       The LPAPI can also be made available "off the shelf" for use in applications  
2 such as web servers (CGI, ISAPI), browsers (Java, ActiveX, plug-ins) and third party  
3 programs such as creativity tools and multimedia development systems.  
4

5       The Toolbox can be used by content owners to interactively create  
6 CONTAINERS. The Toolbox focuses on ease-of-use through an intuitive interface  
7 with on-line help, wizards, and other supporting mechanisms. The Toolbox can  
8 create registered and unregistered CONTAINERS. The Toolbox combines Templates  
9 provided by the Registry for registered objects, or by other means for unregistered  
10 objects. Some Registries can choose to use standard Templates. The Template Editor  
11 is useful, for example, for creators who are using Registries that allow Objects to be  
12 registered with custom templates that are derived from those supplied by the  
13 Registry. This provides the Registry with the capacity to allow creators to add  
14 additional properties that complement those required by the Registry. The Toolbox  
15 can use cryptographic techniques to ensure the integrity of the CONTAINER and to  
16 provide two-way authentication of the parties involved in object registration.  
17

18       Appendix A contains, for disclosure purposes, source code which illustrates  
19 certain operational aspects of the invention. Appendix B contains - for disclosure  
20 purposes, and without limitation to the above-described invention - further  
21 descriptions of alternative and supplemental object-based system parameters which  
22 can be used in accord with the invention.  
23

24       The invention thus attains the objects set forth above, among those apparent  
25 from preceding description. Since certain changes may be made in the above  
26 apparatus and methods without departing from the scope of the invention, it is  
27 intended that all matter contained in the above description or shown in the  
28 accompanying drawing be interpreted as illustrative and not in a limiting sense.  
29